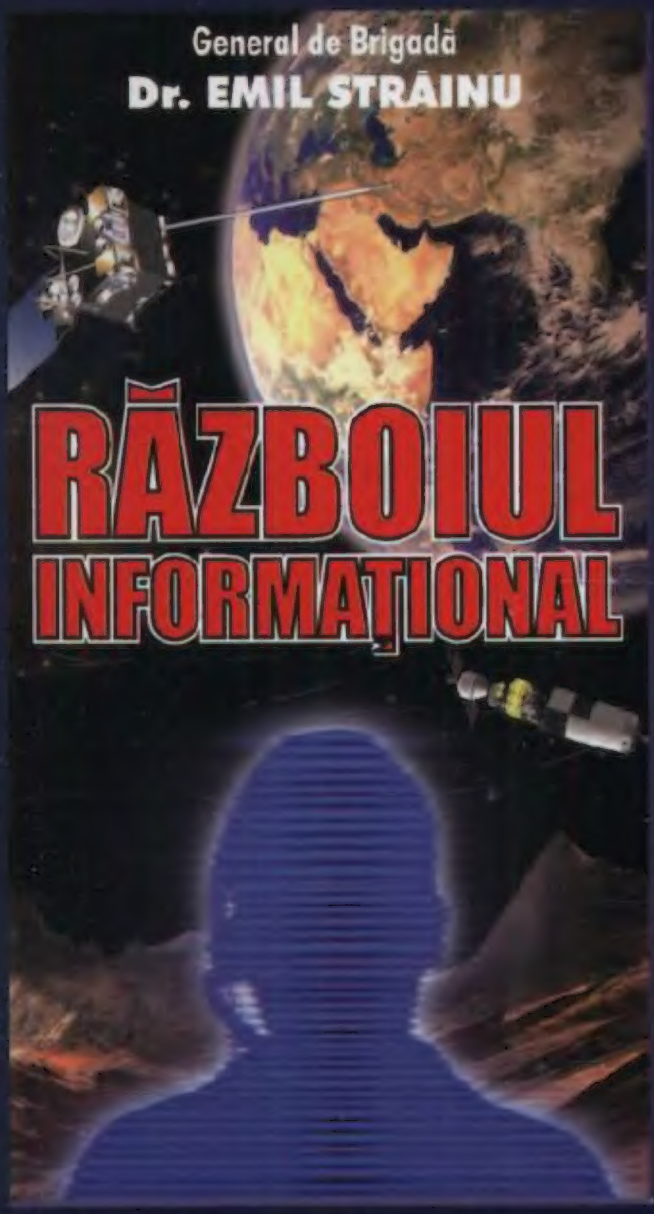
General de Brigadă

Dr. EMIL STRĂINU



RĂZBOIUL INFORMAȚIONAL

General de brigadă dr. Emil Străinu

RĂZBOIUL INFORMAȚIONAL

Mică Enciclopedie

Director: Sorin Chifulescu
Coperta: DEIMOS IMAGE
Redactor: Gabriel Chivu
Tehnoredactor: Adriana Fleancu
Corector: Alexandra Ionescu

Toate drepturile sunt rezervate Editurii **SOLARIS® PRINT.**
Nici o parte din acest volum nu poate fi copiată
fără permisiunea scrisă a Editurii **SOLARIS® PRINT.**
Drepturile de distribuţie în străinătate aparţin,
în exclusivitate, Editurii **SOLARIS® PRINT.**

Cartea prin poştă: editura.solaris@yahoo.com

Descrierea CIP a Bibliotecii Naţionale a României

STRĂINU, EMIL, Războiul Informaţional / Străinu Emil. - Bucureşti : Solaris Print, 2009

ISBN 978-606-92077-3-4

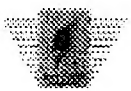
ISBN 978-606-92077-3-4
Copyright© 2009 **SOLARIS® PRINT**

General de brigadă dr. Emil Străinu

RĂZBOIUL INFORMAȚIONAL

Mică Enciclopedie

Coordonatorul lucrării: **Psihosociolog Cornelia Prioteasa**
Consilier Științific: **Prof.univ Gheorghe Butucaru**



Editura SOLARIS PRINT
BUCUREȘTI – 2009

Motto:

O informație pe care o ai nu este cea pe care o vrei
O informație pe care o vrei nu este cea de care ai nevoie
O informație de care ai nevoie nu este cea pe care o poți obține
O informație pe care o poți obține costă mai mult decît poți să plătești

MURPHY (Legile informației)

PREFAȚĂ

Analiza tipurilor de agresiuni* la care a fost/este supusă țara noastră în prezent duce la oncluzia că cel mai grav fenomen cu care ne confruntăm acum (mai grav chiar decît cele din sfera economică) este un ***complex proces de destructurare a realității etnice românești.***

Prin aceste acțiuni se urmărește lovirea și alterarea/ distrugerea celui mai intim și prețios filon al națiunii române – **Ființa Națională**

Autorii sunt state, corporații transnaționale, grupuri și grupări de interese mai mult sau mai puțin oculte, unele acționând la vedere altele în ascuns, chiar și de pe teritoriul național.

Mijloacele de atac sunt unele „domestice" ce acționează „pe față", cum sunt mass-media și internetul cât și altele conspirate ce țin de modul de operare al serviciilor speciale și agențiilor secrete de informații.

Căile de atac sunt cele specifice **războiului informațional, războiului imagologic, războiului psihologic și nu în ultimul rînd războiului psihotronic.**

Pentru cunoașterea și identificarea unora dintre cele mai utilizate forme și procedee de ducere a războiului informațional am strâns în prezentul volum păreri și concepții ale unor specialiști de marcă în domeniu.

Prezenta lucrare are un caracter de referință și adună la un loc unele din cele mai semnificative tendințe și orientări actuale și de perspectivă din domeniul războiului informațional.

---

* Vezi despre agresiuni geofizice (Canalul Bâstroe, de exemplu) agresiuni ce țin de războiul climatic, agresiuni meteorologice, etc.) în **Războiul Geofizic**, Editura Solaris, București 2009, etc. Agresiuni de tip psihotronic în **Războiul Psihotronic** , Editura Solaris , București, 2009.

Oficial, conceptul de război electronic (R.I.) a fost lansat în Statele Unite, în decembrie 1992 (la aproape doi ani de la Războiul din Golf, considerat a fi „războiul pilot" în care s-au folosit mijloace specifice R.I.).

În septembrie 1995, Departamentul Apărării al SUA, a publicat prima definiție oficială a războiului informațional: **„Războiul informațional reprezintă acțiunile întreprinse pentru a obține superioritatea informațională, prin afectarea informațiilor adversarului, a proceselor și sistemelor informaționale, în paralel cu acțiunile întreprinse pentru a apăra propriile informații , procese și sisteme informaționale."**

Multora dintre noi le este încă în minte transmisia în direct a războiului din Golf de către rețeaua de televiziune americană CNN. Dar să nu uităm și de transmisia în direct la Televiziunea Națională a Revoluției Române din Decembrie 1989.

Pentru specialiști, jurnaliști dar și pentru publicul larg prezentul volum deschide noi orizonturi ale cunoașterii realității actuale, confruntate cu numeroase provocări nonconvenționale și asimetrice printre care și cu un nou tip de război: **Războiul Cunoașterii...**

Dr. **Emil Străinu**

BAZELE RĂZBOIULUI INFORMAȚIONAL

ERA INFORMAȚIEI

Ronald R. Fogleman*
Sheila E. Widnall**

Competiția pentru informație este la fel de veche ca și conflictele umane. Este o caracteristică virtual definitorie a umanității. Națiunile, corporațiile și indivizii caută, fiecare, să-și mărească și să își protejeze depozitul propriu de informații, în timp ce încearcă să îl penetreze pe cel al adversarului. Aproximativ din 1970 au avut loc îmbunătățiri extraordinare în mijloacele tehnice de colectare, stocare, analizare și transmitere a informațiilor.

Au fost scrise topuri întregi despre impactul acestei revoluții tehnice asupra conducerii războiului, în special de la ***"Furtuna în Deșert"***. Totuși, majoritatea acestor lucrări se concentrează, în principal, asupra dezvoltărilor tehnice, nu asupra modului în care aceste dezvoltări au impact asupra doctrinei.

Acest material va formula întrebări importante pentru strategii US Army și Air Force și va da răspunsuri ferm bazate pe definiții concise, experiență instituțională și pe concepte doctrinale.

In acest proces se va clarifica de ce competiția pentru informații, care a apărut în zorile istoriei, este dintr-o dată un subiect central al siguranței naționale. Mai aproape de casă, acest domeniu va descrie, de asemenea, modul în care ar trebui să evolueze doctrina Air Force și US Army pentru a face față

---

* General, USAF, Chief of Staff
** Secretary of the Air Force

războiului informațional. Scopul final este o fundamentare serioasă pe care să se bazeze inevitabilele schimbări în organizarea, pregătirea, dotarea și mobilizarea forțelor și capacităților militare. Deoarece are loc o revoluție tehnologică [1] penetrând în forță prin sistemele informaționale și prin integrarea lor în viața noastră de zi cu zi și ducând la termenul ***„Era informației"***.

Tehnologiile legate de informații concentrează date, măresc imens viteza de prelucrare și transmitere a datelor și asociază intim rezultatele în aproximativ orice aspect al vieților noastre. ***Era informației*** transformă toate operațiunile militare prin faptul că furnizează comandanților informații fără precedent din punctul de vedere al cantității și calității [2]. Comandantul, care are avantajul în ceea ce privește observarea spațiului de luptă, analiza evenimentelor și distribuirea informațiilor, posedă un puternic, dacă nu decisiv, avantaj în raport cu adversarul.

Inainte de a continua, trebuie să facem distincția între *războiul epocii informaționale* și *războiul informațional.* Facem această distincție deoarece majoritatea literaturii tratează războiul informațional și progresele în tehnologia informației sinonim.

Războiul epocii informaționale folosește tehnologia informațională ca pe o unealtă de a asigura economii, fără precedent de timp și forțe, în operațiunile noastre de luptă. În ultimă instanță, războiul epocii informaționale va afecta *toate* operațiunile de lupta [3].

---

[1] Baza tehnologică a sistemelor informaționale s-a schimbat radical din 1970. Aceste schimbări includ creșterea capacității de stocare, a vitezei de accesare, vitezei de execuție a instrucțiunilor și vitezelor de comunicare. Datorită acestor schimbări, sistemele informaționale penetrează în viața noastră. Considerăm aceasta ca fiind dovada *prima facie* a unei revoluții. Totuși, acest capitol nu intenționează să răspundă întrebarii daca aceste schimbări constituie o revoluție sau măcar o evoluție.

[2] Aici, conceptul de calitate se referă la oportunitate, specificitate și concretețe.

[3] Rachetele de croazieră exploatează tehnologiile erei informaționale pentru a plasa o bomba la țintă. Acesta este un exemplu de armament al erei informaționale - utilizarea tehnologiei erei informaționale cu mijloace de îndeplinire în conditii mai bune a unei misiuni.

Prin contrast, războiul informațional, subiectul acestui document, vizualizează informația în sine ca pe un domeniu separat, o armă puternică și o țintă operativă.

Informația, după cum vom arăta în cele ce urmează, este dependentă de tehnologie. Totuși, tehnologia erei informaționale transformă în fapte o posibilitate teoretică: manipularea *directă* [4] a informațiilor adversarului. Acesta este firul conducător al acestui document.

CE ESTE INFORMAȚIA? Această întrebare este elementară, dar crucială. Este imposibilă discutarea coerentă despre războiul informațional fără a defini riguros conceptul central: **informația.**

Informațiile derivă din fenomene. Fenomenele, faptele sau evenimentele observabile, sunt *tot* ce se întâmplă în jurul nostru. Pentru a deveni informații, fenomenele trebuie percepute și interpretate. În consecință, informațiile sunt rezultatul a două elemente: fenomenele (datele) percepute și instrucțiunile necesare pentru a interpreta aceste date și a le da sens.

Această distincție este importantă și poate fi ușor sintetizată într-un paradox familiar: dacă un copac cade, dar nu e nimeni în împrejurimi ca să audă această cădere, a făcut zgomot? Copacul în cădere a cauzat unde de presiune în atmosferă, un fenomen. Zgomotul, informația denotând căderea copacului, survine atunci când urechea cuiva detectează undele de presiune, creând date, și instrucțiunile creierului manipulează datele în sunetul care poate fi recunoscut ca un copac în cădere dacă nu există o persoană care să îl audă (sau să îl vadă).

Fenomenele devin informații prin observație și analiză. Prin urmare, informațiile sunt o abstracție a fenomenelor. Informațiile sunt rezultatul percepțiilor și interpretărilor noastre, indiferent de mijloace. După cum exemplifica cu claritate copacul în cădere, definirea informației presupune două caracteristici:

---

[4] Manipularea directă modifică informațiile adversarului, în timp ce ocolește perspectiva adversarului, analitică sau procesul deciziei.

- Informația: *date și instrucțiuni.*

Rețineți că definiția este distinctă pentru informații și pentru tehnologie. Totuși, ce putem face cu informațiile și cât de repede o putem face, este *foarte* dependent de tehnologie. Tehnologia dezvoltă dramatic mijlocele noastre observaționale, dezvoltă și concentrează depozitele de date și accelerează prelucrarea instrucțiunilor. Folosim termenul următor pentru a circumscrie elementele dependente de tehnologie asociate cu informațiile:

- **Funcția informațională:** *orice activitate presupunând achiziția, transmisia, stocarea și procesarea informațiilor.*

De exemplu, sistemul care spune unei mașini să ștanțeze optzeci de capace de butuc realizează o funcție informațională. Presa de metal care le ștanțează nu o face.

După cum s-a menționat anterior, comandantul, având informații mai bune, deține un avantaj asupra adversarului. Operațiunile militare formulează cereri speciale de funcții informaționale, căutând să-i dea comandantului un avantaj informațional.

Supravegherea și recunoașterea sunt puterile noastre de observație. Inteligența și analiza vremii sunt bazele pentru orientarea observațiilor. Folosim aceste baze pentru a forma un "Air Tasking Order", care comandă și conduce operațiunile de execuție și monitorizare în dirijarea conflictului. Navigația de precizie facilitează îndeplinirea misiunii. Impreună, acestea sunt tipurile de funcții informaționale militare care facilitează *toate* operațiunile militare. Folosim termenul colectiv de funcții informaționale militare pentru a descrie funcțiile informaționale de stimulare a forței.

Funcții Informaționale Militare: *orice funcție informațională sprijinind și facilitând mobilizarea forțelor militare.*

Această definiție servește la delimitarea funcțiilor informaționale militare importante de universul total al funcțiilor informaționale.

La nivel de înaltă strategie, națiunile urmăresc să obțină,

exploateze și protejeze informațiile în sprijinul obiectivelor lor. Această exploatare și protecție poate avea loc de exemplu în arenele economice, politice sau militare. Cunoașterea informațiilor adversarului este un mijloc de dezvoltare a capacităților proprii, de degradare sau contracarare a capacităților inamicului și protejare a activelor proprii, *inclusiv propriile informații.*

Asta nu e nou. Efortul de descoperire și exploatare a informațiilor a început de prima dată de când un grup de oameni a încercat să dobândească un avantaj asupra altuia.

Războiul informațional constă din vizarea informațiilor și funcțiilor informaționale ale inamicului, protejându-le pe ale noastre, cu intenția de a deteriora voința sau capacitatea de luptă a acestuia.

Concentrându-ne asupra informațiilor și funcțiilor informaționale, definim războiul informațional ca:

Războiul Informațional: *orice acțiune de refuz, exploatare, corupere și distrugere a informațiilor și funcțiilor inamicului; protecția proprie împotriva acestor acțiuni și exploatarea funcțiilor proprii informaționale militare* [5].

Această definiție este baza următoarelor aserțiuni:

Războiul informațional este orice atac împotriva oricărei funcții informaționale, indiferent de mijloace. *Bombardarea unei centrale telefonice este război informațional. La fel este și distrugerea soft-ului acestei centrale.*

Războiul informațional este orice acțiune de protejare a propriilor funcții informaționale, indiferent de mijloce. *Întărirea și protejarea centralei împotriva atacului aerian este război informațional. La fel este și utilizarea unui program anti-virus pentru protejarea soft-ului instalației.*

Războiul informațional este un mijioc, nu o finalitate, **în exact același mod în care războiul aviatic este un mijloc**, nu o finalitate. *Putem folosi războiul informațional ca un mijloc de dirijare a*

[5] Această definiție depinde numai de natura acțiunii, nu de cum aceasta este realizată.

atacului strategic și interdicției, de exemplu, exact la fel cum putem folosi războiul aviatic pentru a dirija atacul strategic și interdicția.

Militarii au încercat întotdeauna să obțină sau să afecteze informațiile necesare unui adversar pentru a-și mobiliza efectiv forțele. Strategiile trecute se bazau, în mod tipic, pe măsuri de genul disimulare și diversiune [6] pentru a influența deciziile, afectând percepțiile factorilor de decizie. Deoarece aceste strategii au influențat informațiile prin procesul de percepție, ele atacau *indirect* informațiile inamicului. Adică, pentru ca diversiunea să fie eficientă, inamicul trebuia sa facă trei lucruri:

- să observe diversiunea;
- sa o analizeze ca realitate;
- să acționeze în baza ei, conform scopurilor, pentru care diversiunea a fost realizată.

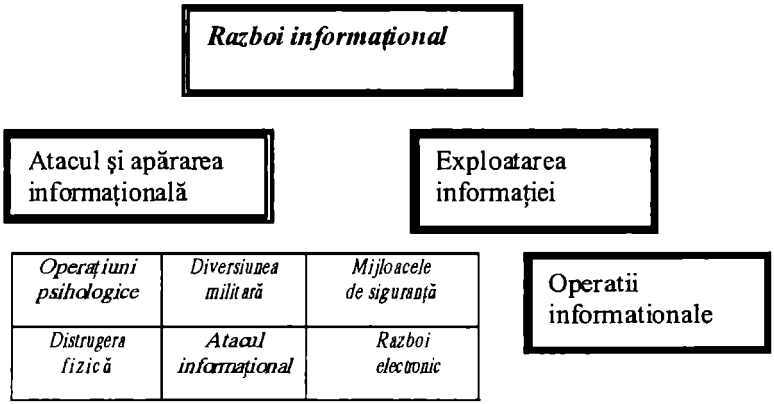
Totuși, mijloacele moderne de realizare a funcțiilor informaționale conferă informațiilor un plus de vulnerabilitate: accesul și manipularea directă.

Tehnologia modernă permite acum unui adversar să schimbe sau să creeze informații fără a se baza pe observare și interpretare. Iată o scurtă listă de caracteristici ale sistemelor informaționale moderne creând această vulnerabilitate: stocarea concentrată, viteza de accesare, transmiterea dispersată a informațiilor și capacitatea sporită a sistemelor informaționale de a dirija acțiuni într-o manieră autonomă. Măsurile inteligente de securitate pot reduce, dar nu pot elimina această vulnerabilitate; absența lor o face frapantă.

Militarii nu sunt înclinați să încredințeze succesul lor în lupta norocului. Deci trebuie să ne dirijăm eforturile în războiul informațional spre mai mult decât vizarea informațiilor adversarului: trebuie și să ne protejam informațiile și toate

[6] Repetăm: Războiul informațional indirect: A schimba informația adversarului prin crearea de fenomene pe care adversarul trebuie să le observe și să le analizeze. Războiul informațional, când este folosit pentru a degrada abilitățile adversarului în fenomene viitoare exacte, conduce la războiul informațional indirect.Războiul informațional direct: A schimba informația adversarului prin crearea de fenomene fară a implica intervenția funcțiilor perceptive și analitice.

operațiunile aferente. Air Force depinde esențialmente de funcțiile informaționale militare, ceea ce ne face vulnerabili la agresiunea informațională. Integritatea funcțiilor noastre informaționale militare, ca și a informației în sine, depinde esențialmente și în manieră directă de succesul operațiunilor noastre militare.



Reamintindu-ne definiția, războiul informațional constă din activități care refuză, exploatează, corup, distrug sau protejează informațiile. Mijloacele tradiționale de realizare a războiului informațional includ operațiunile psihologice, războiul electronic, diversiunea militară, atacul psihologic și diversele măsuri de securitate.

Operațiunile psihologice *folosesc informațiile pentru a afecta raționamentul inamicului.*

Războiul electronic *refuză inamicului informații corecte.*

Diversiunea militară *induce inamicul în eroare în ceea ce privește capacitățile sau intențiile noastre*[7].

[7] Diversiunea militară dă un excelent exemplu de cum acțiunile sunt definite de finalitățile lor nu de mijloace. Puterea aeriană poate conduce războiul informațional prin diversiunea militară ca în operațiunea "Fortitude North", din al doilea Război Mondial, unde persoane neidentificate au detonat două bombe în Pas de Calais, pentru fiecare bombă aruncată în Normandia, un efort de succes în inducerea în eroare a nemților în ceea ce privește planurile noastre de invazie.

Distrugerea fizică *poate realiza războiul informațional prin afectarea elementelor sistemului informațional prin conversia energiei stocate în energie distructivă. Mijloacele de atac fizic variază de la bombe convenționale până la arme cu impulsuri electromagnetice.*

Mijloacele de siguranță *urmăresc să împiedice adversarul să afle despre capacitățile și intențiile noastre în plan militar*[8].

Era informației a prevăzut mijloace noi și practice pentru a refuza, exploata, corupe sau distruge informația, la fel ca vulnerabilitățile ce fac aceste atacuri posibile. Doctrina US Army și Air Force nu cunoaște și nu definește aceste atacuri asupra informației, pe care noi le numim *'atacul informațional'*.

Atacul informațional *degradarea directă a informației fără schimbări vizibile a entității acesteia înăuntrul căreia se află.*

Atacul informațional, constrâns de definiția informației, este limitat la modificarea directă a datelor și instrucțiunilor. Este, prin urmare, tocmai un alt mijloc de conducere a războiului informațional, unul a căror efecte imediate nu include schimbări vizibile a entității înăuntrul căreia aceasta se află.

Ca să spunem așa, după ce a devenit subiectul atacului informațional o funcție informațională nu se poate distinge de starea ei originală, decât prin verificarea datelor și instrucțiunilor sale [9].

Așa cum am descris anterior, există două căi de a influența funcțiile informaționale ale adversarului: directă și indirectă.

Războiul informațional indirect afectează informația creând fenomene, pe care adversarul la va percepe, interpreta și acționa asupra lor.

Diversiunea militară, atacul psihic și dezinformarea tradițională își ating țelurile indirect. De exemplu, ținta decepției este de a determina adversarul să ia decizii incorecte; decepția reușind acest lucru prin crearea unei realități aparente.

---

[8] Măsurile de securitate curente includ OPSEC, COMSEC și COMPUSEC. Ca evoluție a tehnologiei informaționale, aceste măsuri de securitate mai mult ca sigur vor evolua în forme total diferite.

[9] Aruncarea unui magnet puternic, de catre o echipă SOF asupra unui hard disc este un exemplu de atac informațional.

În general, această substituție crează fenomene pe care inamicul trebuie să le observe. Reușita, oricum, depinde de câteva condiții: adversarul, în realitate să observe fenomenul și ulterior să îl transforme în date; să-l analizeze în informația dorită și să acționeze în baza informației, în maniera dorită.

Războiul informațional direct afectează informația prin modificarea componentelor sale, fără a se baza pe puterile adversarului de percepere și interpretare. Atacul informațional acționează direct asupra informației adversarului. De curând toate funcțiile informaționale sunt însăși controlate de informație, atacul informațional putând fi direct împotriva celor mai multe funcții informaționale.

Războiul informațional direct, centrul atacului informațional, acționează asupra informațiilor adversarului, fără a se baza pe funcțiile de culegere, analiză și decizie ale lui. Poate scurtcircuita bucla OODA[10] (Observație, Orientare, Decizie și Acțiune) prin crearea unor observații și perturbării orientării, sau o poate decapita prin impunerea unor decizii sau provocarea unor acțiuni. O scurtă ilustrare va servi pentru a demonstra diferența între aplicațiile războiului informațional direct și indirect:

Scopul nostru, folosind diversiunea militară, este să facem adversarul să creadă că există o escadrilă de aparate de luptă acolo unde de fapt, nu este nici una, și să acționeze, în baza acestei informații, într-o manieră benefică pentru operațiunile noastre.

Războiul informațional indirect: folosind diversiunea militară, putem construi piste false și hangare false, și să generăm alte activități suficiente pentru a prezenta o imagine convingătoare. Ne bazăm pe adversar să observe pseudo-operațiunile de luptă și să le interpreteze că fiind reale (contrar detectării lor ca false). Doar atunci aceasta devine informația pe care vrem ca adversarul să o aibă.

[10] OODA: Observatie, Orientare, Decizie si Acțiune. Observația transformă fenomenele în date. Orientarea procesează datele în informații. Decizia transformă informația în ordine. Acțiunea transformă ordinele în acțiune. Bucla OODA este continuă - atunci când acționezi observi rezultalele începând procesul din nou.

Războiul informațional direct: În sens contrar, dacă folosim atacul informațional pentru a crea escadrila de luptă în baza de informații a adversarului, rezultatul - decepția - este precis același. Dar mijloacele acestui rezultat, care depind de resurse, timp și nesiguranță, sunt dramatic diferite.

Latura defensivă a măsurilor de securitate a războiului informațional vizează protejarea informației (previne ca un adversar să conducă cu succes războiul informațional împotriva funcțiilor noastre informaționale). Măsurile de securitate curente ca OPSEC și COMSEC sunt mijloace tipice de prevenire, detectare și răsturnare a acțiunilor indirecte ale adversarilor asupra funcțiilor noastre informaționale.

In contrast, măsurile de securitate ca COMPUSEC includ prevenirea, detectarea și răsturnarea acțiunilor informaționale directe asupra funcțiilor noastre informaționale. Măsurile de securitate viitoare trebuie să evolueze în raport cu progresele tehnologiei informaționale. Consecutiv, noi măsuri vor lua probabil forme total diferite, de măsurile de securitate de astăzi, înrădăcinate în cerințele de securitate anterioare.

Așa cum demonstrează exemplul simplu din această lucrare, trebuie să evităm să cădem victima efectelor profunde și păgubitoare ale războiului informațional.

Din două motive. În primul rând, pentru că războiul informațional oferă mijloace importante pentru îndeplinirea misiunilor forțelor aeriene, în al doilea rând, pentru că integrarea larg răspândită a sistemelor informaționale în operațiile forțelor aeriene transformă funcțiile noastre informaționale militare într-o țintă valoroasă. Un exemplu ipotetic folosind atacul informațional arată cum războiul informațional poate îndeplini o misiune tipică Air Force:

Interdicția împiedică sau întârzie ajungerea resurselor esențiale la unitățile combatante. În acest sens, o abordare constă în distrugerea podurilor de legătură folosind bombe ghidate cu laser. Ca alternativă, am putea să alterăm informațiile logistice

ale adversarului, marcând în mod intenționat eronat acele poduri ca fiind distruse, ceea ce determină factorii de planificare să redirijeze forțele și resursele. Ambele modalități realizează același scop; atacul informațional oferă posibilitatea de a ne expune activele unui atac.

Ca exemplu, evidențiind necesitatea unei apărări robuste împotriva unei agresiuni informaționale, imaginați-vă haosul care ar apare dacă un adversar ar reuși să penetreze baza noastră de date cu alocare în timp a forțelor. Schimbări subtile în ea ar fi suficiente pentru a reduce aproape la zero capacitățile noastre de protecție.

În prezent, doctrina US Army și Air Force recunoaște războiul aerian și războiul spațial. Totuși, doctrina nu identifică misiuni separate pentru războiul aviatic sau războiul spațial, în loc de asta, ambele interferează rolurile și misiunile. Similar războiul informațional nu poate fi clasificat ca o misiune singulară. A face aceasta ar însemna un eșec pentru integrarea completă a războiului informațional în doctrina forțelor aeriene.

Să ne amintim că misiunile sunt sarcini operaționale îndeplinite pentru obținerea obiectivelor militare. Războiul aerian este un mijloc, definit de mediu, pentru executarea acelor misiuni. Există trei obiective ale războiului aerian:

- controlul spațiului aerian în timp ce protejăm forțele noastre de acțiunile inamicului;
- exploatarea controlului aerian pentru angajarea forțelor proprii împotriva inamicului și sporirea generală a eficienței forțelor noastre.

În doctrina noastră, obiectivele controlului, exploatarea cât și sporirea eficienței se transpun în rolul spațiului aerian, în acțiunea și sporirea forțelor. În multe privințe, informația poate fi considerată ca un domeniu [11] așa cum sunt uscatul, marea, aerul și spațiul.

[11] Regiune, sferă sau domeniu înăuntrul căruia orice se poate întâmpla, predomina sau domina.

Informația are caracteristicile[12] sale proprii de mișcare, greutate și topografie așa cum spațiul, aerul, marea și uscatul au trăsăturile lor distincte. Există paralele conceptuale puternice între conceperea aerului și informația ca domeniu.

Inaintea fraților Wright, aerul, care evident exista, nu era un teren propice pentru operațiuni militare practice și de anvergură. Similar, informațiile existau înainte de epoca informațională. Dar epoca informațională a schimbat caracteristicile domeniului informației ca operațiunile militare de anvergură din interiorul ei să devină practice.

Războiul informațional ca și războiul aerian este mijlocul definit de domeniul în care urmează să fie executate misiunile militare. Există trei obiective ale războiului informațional:

- controlul domeniului informațional în așa fel încât să-l putem exploata în timp ce protejăm funcțiile noastre informaționale militare, de acțiunile inamicului:
- exploatarea controlului informațional pentru angajarea războiului informațional împotriva inamicului;
- sporirea generală a eficacității forțelor prin dezvoltarea deplină a funcțiilor informaționale militare.

Primul obiectiv al războiului informațional, de a controla domeniul pentru ca să îl putem exploata în timp ce protejăm funcțiile noastre informaționale militare de acțiunile inamicului, are o contribuție semnificativă la controlul spațiului de luptă.

În prezent, doctrina forțelor aeriene recunoaște două misiuni pentru controlul spațiului de luptă: antiaeriană și antispațială. Misiunile antiaeriene au ca obiective controlul aerului; misiunile antispațiale au ca obiectiv controlul spațiului. Claritatea și consistența ne cer să numim acele activități, dedicate controlului informațional, contrainformații.

[12] Pământul, marea, aerul și spațiul sunt domenii înăuntrul carora noi putem desfășura operații militare. Fiecare domeniu înăuntrul său impune asupra operațiilor caracteristicile sale. Informația și funcțiile sale, de asemenea, poate fi gazdă pentru operațiile militare, însă aceste operațiuni trebuie să se conformeze cu caracteristicile sistemului informațional și funcțiilor sale.

Contrainformația: *acțiune dedicată pentru a controla spațiul informațional.*

În plus, contrainformația, la fel ca misiunile antiaeriene și antispațiale, are atât aspecte ofensive cât și defensive. Contrainformația ofensivă, ne face capabili să folosim domeniul informațional și îl face pe adversar incapabil sa-l folosească.

Mijloacele tipice includ, atacul fizic, diversiunea militară, operațiile psihologice, războiul electronic și atacul informațional. Contrainformația defensivă, include atât acțiuni active cât și pasive pentru a ne proteja de acțiunile războiului informațional ale adversarului. Ea este realizată, de exemplu, prin apărarea fizică, securitatea fizică, OPSEC, COMSEC, COMPUSEC și serviciile de informații.

Controlul aerospațial ne face capabili să folosim teritoriul aerului și spațiului fără să suferim pierderi substanțiale și să producem pagube însemnate inamicului ce deține aceste teritorii. Contrainformația în colaborare cu misiunile antiaeriene și antispațiale caută să creeze un astfel de mediu.

Al doilea obiectiv al războiului informațional este să exploateze controlul nostru asupra informației, în aplicarea războiului forțelor aeriene, misiunile de atac strategic, interdicția și susținerea aeriană exploatează controlul aerian. Similar războiul informațional ar putea fi folosit să realizeze aceleași obiective. Am citat deja un exemplu despre felul în care războiul informațional poate realiza interdicția. El, de asemenea, poate realiza atacul strategic.

Să presupunem că vrem să limităm mobilitatea pe termen lung a inamicului prin restricționarea aprovizionării cu combustibil. În primul rând, îi identificăm rafinăriile, ca cea mai convenabilă țintă de realizare a acestui țel.

Prin cercetare, identificăm în continuare rafinăriile specifice care au cea mai mare capacitate de producție. La fiecare rafinărie găsim că există un turn de cracare critică. Organizăm o lovitură și cu o admirabilă economie de forță, realizăm scoaterea din

funcțiune a rafinăriilor prin distrugerea numai acelor turnuri în timp ce lăsăm restul neatins. Acesta este un exemplu clasic de atac strategic.

Aceeași situație. Ca în toate rafinăriile moderne și acestea au vaste sisteme de control automat. Aceste funcții informaționale vaste oferă o țintă potențială pentru războiul informațional. La începutul conflictului, noi am realizat o misiune contrainformativă ofensivă prin penetrarea și caracterizarea sistemului de control automat al rafinăriei.

În acest proces, am descoperit câteva puncte informaționale vulnerabile, care ne-au ajutat să stabilim mijloacele pentru afectarea operațiunilor rafinăriilor, la o dată care rămâne la alegerea noastră. Mai târziu, în timpul conflictului, combinat cu interdicția și operațiunile de la sol, alegem să exploatăm una dintre vulnerabilități. In acest fel, am scos din funcțiune rafinăriile lor. Și acesta este un exemplu clasic de atac strategic.

Tehnologia informațională este deja puternic înglobată în operațiunile noastre militare, punând la dispoziție cantități inimaginabile de informații. Exploatând aceste informații avem la dispoziție posibilități de lovire; bazându-ne pe acestea se creează inevitabil vulnerabilități, potențiale deformații. Aceasta, combinată cu progresele atât în abilitate cât și în localizarea și distrugerea punctelor de comandă și control (C2), fac C2 mai mult ca oricând o țintă realizabilă.

Istoria a arătat că operațiunile militare de succes pot realiza lovituri eficiente prin paralizarea abilității inamicului de a exercita comanda și controlul. Aviatorii l-au considerat, întotdeauna un obiectiv important și au depus eforturi mari împotriva C2in aceste două motive, eforturile pentru perturbarea și distrugerea elementelor de comandă și control ale adversarului ne-au determinat să identificăm o misiune separată în aplicațiile forțelor.

Atacul C2: *orice acțiune împotriva oricărui element al sistemului de comandă și control al inamicului.*

Al treilea obiectiv al războiului informațional este dezvoltarea funcțiilor informaționale pentru sporirea eficienței tuturor forțelor. Anterior am descris funcțiile informaționale militare ca un sprijin pentru angajarea forțelor militare.

Doctrina noastră curentă nu include o astfel de misiune. Pentru a umple acest spațiu gol, vom include operațiile informaționale în sporirea forțelor. Câteva exemple de operații informaționale sunt: supravegherea, recunoașterea, comanda și controlul, comunicațiile, identificarea conflictelor, inteligența, precizia zborului și vremea.

Trăsătura distinctă a misiunilor operațiunilor informaționale este că se ocupă în primul rând cu informațiile atât ca resurse cât și ca produs.

Rolul și misiunile puterii aerospațiale			
Controlul aerospațial	Misiuni ale forțelor	Sporirea forțelor	Sprijinul forțelor
Antiaerian	Atacul strategic	Transportul aerian	Baze OPS & DEF
Antispatial	Interdictia	Alimentarea în aer	Logistica
Contra -informatiile	Sprijinul aerian	Transportul în spațiu	Sprijinul
	Atacul C2	Operații speciale	Operational
		Operații informaționale	Sprijinul pe orbită

Operațiile informaționale: *orice acțiune presupunând achiziția, transmisia, stocarea și procesarea informațiilor ce sporesc angajarea de forțe militare.*

Deoarece avem nevoie de informații relevante, veridice și oportune pentru tot ceea ce facem, operațiile informaționale susțin conducerea misiunilor pe parcursul tuturor celor patru roluri, de la controlul aerospațial la sprijinul forțelor.

Operațiile informaționale asigură comandanților abilitatea să observe spațiul de luptă, analiza evenimentelor și forțele directe. Operațiile informaționale asigură logisticienilor abilitatea de a cunoaște ce este în dotare și unde este necesar. Operațiile informaționale asigură conducerea zborului, abilitatea de a

cunoaște unde este ținta, cum este apărarea ei și să selecteze care este cea mai corespunzătoare armă.

In final războiul informațional se interferează cu toate rolurile și misiunile forțelor aeriene. Este un alt mijloc de conducere a misiunilor noastre tradiționale. Oricum există trei sarcini operaționale superioare prin care războiul informațional ne face capabili sa executăm, ceea ce nu este convenabil tratat de către doctrina noastră actuală: contrainformația, Atacul C2 și operațiile informaționale.

Similar, am hotărât să excludem două misiuni care nu mai sunt relevante potrivit regrupărilor misiunilor: războiul electronic, anterior cuprins în cadrul creșterii forțelor, care este acum însumat de către războiul informațional; supravegherea și recunoașterea ce sunt considerate, acum, momente ale operațiilor informaționale.

Oricum, această listă nu este exhaustivă. Așa cum am arătăt titlul acestui material, ideile conținute vizează bazele și nu întreaga construcție. Invariabil, pe măsură ce forțele aeriene se acomodează în totalitate cu revoluția tehnologiei informaționale, se pot ridica sarcini operaționale adiționale care la rândul lor vor adăuga sau exclude unele misiuni.

In sens larg, aceste baze continuă să ofere un test veridic pentru războiul informațional, toate noile misiuni având nevoie să îl susțină și să îl treacă.

Focarul războiului informațional este orice funcție informațională indiferent dacă este C2, un sistem de control al unei rafinării sau o centrală telefonică. C2 reprezintă numai o parte a universului funcțiilor informaționale militare. Statul Major definește comanda și controlul:

> **Comanda și controlul:** ***exercitarea autorității și direcției, de către un comandant corespunzător desemnat asupra forțelor distribuite în îndeplinirea misiunii.***

Comanda și controlul războiului (C2W) se adresează activităților directe împotriva abilității adversarului de a direcționa

dispunerea și angajarea de forțe, sau acelora care protejează prietenoasa amabilitate a comandanților să facă aceasta. Așa cum am arătat, războiul informațional nu atacă numai procesul C2 ci, de asemenea, puterea de luptă însăși a inamicului.

Cu alte cuvinte, prin definiție, C2W nu este asociat cu reducerea sau anularea abilității sau dorinței unităților de luptă de a executa ordinele lor. Operațiile psihologice tactice și contramăsurile electronice de autoprotecție afectează abilitatea unităților să execute ordinele.

Dar ele, în nici un caz, nu afectează abilitatea comandanților să emită ordine acelor unități și nici abilitatea lor de a primi acele ordine. Deși extraordinar de importantă, politica de comandă și control a războiului este numai o aplicație particulară a războiului informațional.

Pentru ca militarii să se concentreze numai asupra C2W, ar trebui să ignore alte ținte legitime. Pentru aceasta războiul informațional și activitățile lui ajutătoare instruirea și aspectele de dotare, sunt esențiale ca C2W să fie deplin eficient.

Noi am stabilit că războiul informațional este important pentru forțele aeriene din două motive. In primul rând, de când funcțiile noastre informaționale militare reprezintă o țintă valoroasă noi trebuie să facem eforturi importante de apărare. În al doilea rând, cum exemplele din această lucrare arată că războiul informațional este un mijloc potențial de realizare a misiunilor tipice forțelor aeriene: atacul strategic, interdicția etc. Mai temeinic forțele aeriene deja produc războiul informațional prin sisteme cum sunt EF-111 și "Compass Call".

Dar, într-un sens mai larg, războiul informațional ar putea fi un mijloc de conducere a oricărei misiuni pe care serviciul deja o exercită - serviciul este în cea mai buna poziție, ca să aleagă mijloacele cele mai bune pentru finalizarea lor. Fiecare serviciu are cerințele sale operaționale unice.

În cele din urmă armata este cea mai calificată să decidă care mijloace sunt cele mai corespunzătoare pentru atingerea scopurilor

pe care comandantul Statului Major le-a stabilit pentru armată. Ca un rezultat al expertizei unice a serviciului cerințele proprii OODA, logisticii etc., fiecare serviciu are preocupări pentru războiul informațional. În dezvoltarea construcției doctrinale în acest material am folosit terminologia și exemplele forțelor aeriene.

Acesta este fondul nostru, aceștia sunt termenii și spațiul cu care suntem obișnuiți. Dar argumentul pe care noi îl prezentăm nu este dependent de terminologie, înlocuirea termenilor forțelor aeriene, cu cei ai armatei ori ai marinei vor lăsa concluziile neschimbate.

CONCLUZII: Revoluția informațională, care a apărut rapid, nu arată semne de încetineală. In măsura in care forțele aeriene devin mai sofisticate din punct de vedere tehnologic, în aceeași măsură devin dependente tehnologic. Trebuie să folosim această sofisticată tehnologie pentru a beneficia de toate oportunitățile pe care informația le oferă ca țintă.

De asemenea, trebuie să fim conștienți că echipamentele noastre tehnice pot reprezenta o posibilă deformație vulnerabilă. Sistemele noastre robuste de apărare ale funcțiilor informaționale pot reprezenta ceea ce ne face pe noi sa nu fi întâmpinat eșecuri militare.

Informația, combinată cu funcțiile informaționale, are trăsături distincte care garantează ca să fie considerată un domeniu, la fel cum uscatul, marea, aerul și spațiul sunt domenii.

Războiul informațional nu ocupă un loc minor în doctrina forțelor aeriene. La fel ca războiul aerian, războiul informațional poate face parte din multe misiuni AFM 1-1. La fel ca atunci când războiul spațial a fost integrat in doctrina forțelor aeriene, tratarea informației ca un domeniu, ne dă posibilitatea, acum, să adăugăm alte misiuni:

Contrainformația: Acțiune dedicată pentru a controla spațiul informațional.

Atacul C2: Orice acțiune împotriva oricărui element al sistemului de comandă și control a adversarului.

Operațiile informaționale: Orice acțiune presupunând achiziția, transmisia, stocarea sau procesarea informațiilor care implică mobilizarea forțelor militare.

De la primul Război Mondial, aviatorii au trebuit să controleze efectiv spațiul aerian pentru a angaja puterea aeriană. Mai mult, superioritatea în aer și spațiu este virtual "sine gua non" pentru angajarea forțelor terestre și navale. Informația este următorul domeniu pe care trebuie să-l controlăm pentru a opera eficient și cu cea mai mare economie de forțe.

La începui am arătat că lupta pentru informații este atât de veche ca primul conflict uman. Ea implică creșterea și protecția stocului nostru de informații și timp ce le penetrează și limitează pe cele ale adversarului.

Recenta explozie în tehnologia informațională îndeamnă punerea în discuție a războiului informațional în și din afara guvernului, țintind funcțiile informaționale ale inamicului, în timp ce le protejează pe ale noastre, cu intenția de degradare a voinței și capacității sale de luptă.

Pentru aviatori, controlul spațiului de luptă este misiunea nr.1. Odată cu progresele în tehnologia informațiilor, aviatorul trebuie să dovedească superioritatea în informații așa cum au superioritate în aer și spațiu.

Numai cu aceste domenii sub controlul nostru putem efectiv angaja activele noastre. Funcțiile informației militare sunt esențiale pentru operațiunile noastre de luptă, ele sunt un instrument de realizare a obiectivelor comandantului Forțelor Unite. Țintind funcțiile informaționale ale adversarului îl împiedicăm să și le realizeze.

În această lucrare am expus buzele doctrinei războiului informațional. Scopul nostru este să oferim o bază larg acceptată pentru adoptarea doctrinei forțelor aeriene la epoca informațională. Ultima țintă? Să încorporam războiul informațional în felul în care Air Force organizează, antrenează, echipează și acționează.

Definiții

• **Atacul C2**: Orice acțiune împotriva oricărui element al sistemului de comandă și control al adversarului.

• **Comandă și control**: Exercitarea autorității și direcției, de către un comandant corespunzător desemnat asupra forțelor distribuite în îndeplinirea misiunii.

• **Contrainformația**: Acțiune dedicată pentru a controla spațiul informațional.

• **Contrainformația defensivă**: Acțiune ce protejează funcțiile noastre militare de adversar.

• **Războiul informațional direct**: A schimba informația adversarului prin crearea de fenomene fără a implica intervenția funcțiilor perceptive și analitice.

• **Războiul informațional indirect**: A schimba informația adversarului prin crearea de fenomene pe care adversarul trebuie să le observe și să le analizeze.

• **Informația**: Date și instrucțiuni.

• **Atacul informațional**: Degradarea directă a informației fără schimbări vizibile a entității acesteia, înăuntrul căreia se află.

• **Funcția informațională**: Orice activitate presupunând achiziția, transmisia, stocarea și procesarea informațiilor.

• **Operațiile informaționale**: Orice acțiune presupunând achiziția, transmisia, stocarea sau procesarea informațiilor care implică mobilizarea forțelor militare.

• **Război informațional**: Orice acțiune de refuz, exploatare, corupere și distrugere a informațiilor și funcțiilor inamicului; protecția proprie împotriva acestor acțiuni și exploatarea funcțiilor informaționale militare.

• **Funcții informaționale militare**: Orice funcție informațională sprijinind și facilitând mobilizarea forțelor militare.

Contrainformația ofensivă: Acțiune împotriva funcțiilor informaționale ale adversarului.

RĂZBOIUL INFORMAȚIONAL DEFENSIV

DAVID S. ALBERTS*

Războiul informațional a devenit sinonim cu revoluția în tehnologiile informaționale și cu potențialul acestora de a transforma strategii militare și capabilități. Există un consens în privința ideii potrivit căreia prosperitatea națională, dacă nu chiar supraviețuirea, depinde de abilitatea noastră de a dezvolta efectiv tehnologia informațională. Fără să fim capabili să apărăm informația vitală, procesele și sistemele informaționale, o astfel de strategie este sortită eșecului.

RI este adesea considerat ca fiind definit de un set particular de ținte – factori de decizie, informație, procese și sisteme informaționale. Asocierea spațiului de conflict („battlespace") și a RI este în constantă creștere, depășind situațiile militare tradiționale. În unele medii, RI este asociat cu creșterea tehnologiilor informaționale, pentru a obține o eficiență sporită.

Acest lucru a lărgit la maxim înțelesul conceptului de RI și a semănat multă confuzie. Pentru acest motiv, în materialul de față, sintagma „strategii informaționale" se referă la recunoașterea și utilizarea informației și tehnologiei informaționale ca instrument de putere națională, care poate fi independent de, sau complementar cu, prezența și operațiile militare.

Întinderea sau spațiul de conflict, al strategiei RI, poate fi definită de jucători și de cele trei dimensiuni - natura, nivelul și zonele interacțiilor lor (Figura 1). Statele nu sunt singurii jucători. Actorii non-statali (grupuri politice, etnice și religioase, crima

* Institutul de Studii Naționale Strategice, Universitatea Națională de Apărare Washington D.C.

organizată, organizații internaționale și transnaționale, persoane care au acces la tehnologia informațională etc.) sunt apți să angajeze atacuri informaționale și să dezvolte strategii informaționale pentru a-și atinge scopurile. În ultima vreme, termenul de „război" a fost folosit destul de neglijent (exemple: Războiul Sărăciei, Războiul Drogurilor, Războiul Crimei), însă acest lucru nu trebuie să surprindă. RI a evoluat în ultimii ani și a devenit un termen atotcuprinzător, referindu-se la activități disparate, unele dintre ele fiind de mult timp asociate ideii de competiție, de conflict și de război.

Acestea includ activități mergând de la campanii de propagandă (incluzând războiul mass-mediei) la atacuri (fizice sau nu) contra comandanților, surselor lor de informare, și mijloacelor de comunicare cu forțele lor. Sub această umbrelă largă, cunoscută ca fiind RI, putem găsi activități ce sunt asociate cu concepte și operații militare, incluzând înșelătoria, războiul de comandă și control (C2W) și operații psihologice (Psyops). Progresele tehnologice au adăugat noi forme de război: războiul electronic (EW) și războiul hackerilor.

Termenul de „Război informațional defensiv" (RI-D) se referă la toate acțiunile întreprinse pentru a se apăra împotriva atacurilor informaționale (atacuri asupra factorilor de decizie, informației, proceselor informaționale și mijloacelor de comunicare a deciziilor lor). În sens strict, din moment ce aceste atacuri pot fi lansate pe timp de pace către ținte civile de către grupuri care nu sunt militare, atât străine cât și autohtone, în loc de RI-D ar trebui să se utilizeze termenul de „Strategie a Războiului informațional defensiv".

Această privire de ansamblu, asupra RI-D, nu încearcă să rezolve problemele apărării împotriva diferitelor tipuri de atacuri informaționale, ci mai degrabă dorește să focalizeze atenția pe subsetul RI, care implică atacuri asupra structurii noastre informaționale, incluzând ceea ce a devenit cunoscut ca fiind „războiul hackerilor", și în forma sa mai serioasă, „războiul digital".

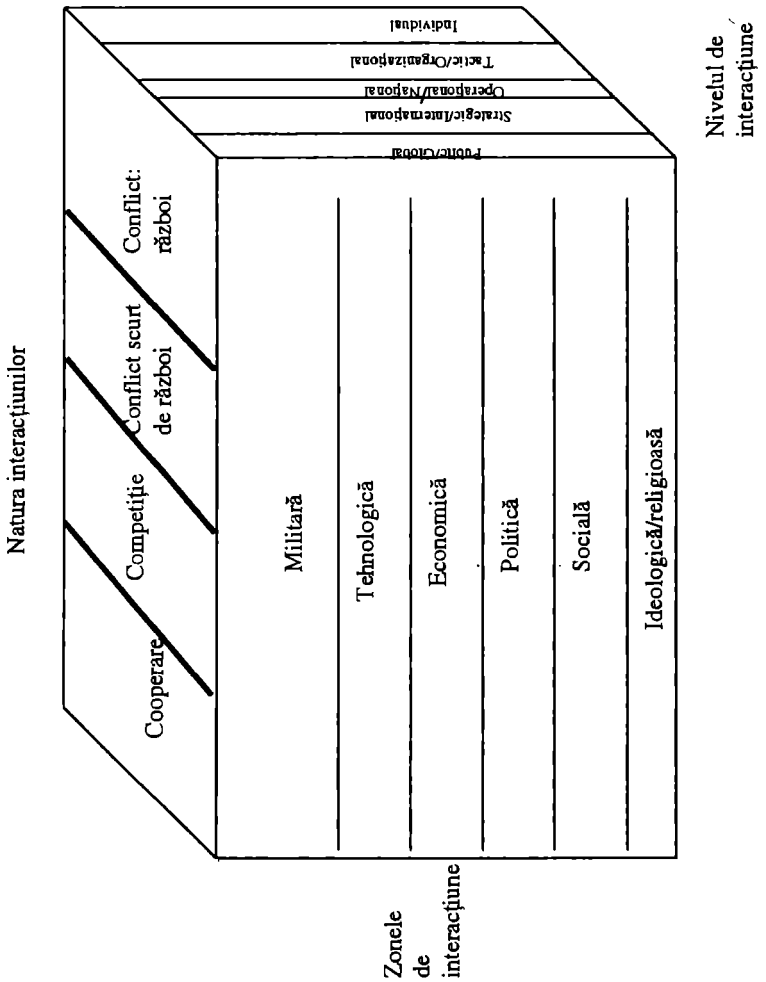


Figura 1. Domeniul Strategiei Războiului informațional

Apărarea împotriva atacurilor informaționale are câteva caracteristici în comun cu eforturile societății de a combate boala, drogurile și crima. Notarea acestor similarități ne ajută să încadrăm problema, să oferim câteva lecții utile și să ne servim de o unitate de măsură.

Înainte de a trece în revistă câteva similarități dintre combaterea RI-D și aceste probleme mai vechi, trebuie spus că, în timp ce eradicarea atacurilor informaționale nu poate fi o așteptare realistă, progrese semnificative pot fi făcute în apărarea contra tuturor tipurilor de atac, astfel că riscurile pot fi menținute la nivelurile acceptabile. A ne apăra include posibilitatea de a preveni atacuri, de a face inofensive atacurile și de a controla pagubele cauzate de acestea.

Problema RI-D este similară cu problemele întâlnite în eforturile de combatere a bolilor, drogurilor și crimei. În primul rând, soluționarea oricăreia dintre aceste probleme necesită eforturi din partea unui anumit număr de organizații publice și private.

În al doilea rând, este puțin probabil, dată fiind competiția pentru resurse, ca vreunul dintre aceste eforturi să fie sponsorizat în totalitate. De aceea, ne putem aștepta să nu fie asigurat niciodată un nivel suficient de sponsorizare a programelor RI-D, așa cum spun că ar trebui, cei care sunt responsabili cu problema RI-D.

În al treilea rând, acestea nu sunt probleme statice. Cartelurile de droguri și criminalii cu siguranță învață din greșelile lor. Chiar și virușii învață. De aceea, forțele de apărare sunt nevoite să țină pasul cu atacanții.

În al patrulea rând, conștientizarea și implicarea publică vor atinge apogeul doar acompaniate de mari eforturi pentru soluționarea problemei. Aceste scurte perioade de interes vor fi urmate de lungi perioade, în care graba de a soluționa problema va face loc apatiei. A menține sponsorizarea și progresul, în perioadele de încercare de câștigare a interesului public, va fi una dintre principalele provocări din această zonă.

În al cincilea rând, organizațiile și indivizii vor învăța să-și

ajusteze comportamentul pentru a trata problema atacurilor RI și a consecințelor lor nedorite.

În sfârșit, soluțiile vor presupune compromisuri. Acest lucru este datorat tensiunilor naturale care există între numeroșii deținători de mize. Tensiunile dintre întărirea legii și protecția libertăților civile sunt câteva exemple clasice, care au apărut în domeniul informațional.

Atacurile asupra sistemelor informaționale sunt deja un fapt curent în viața de zi cu zi, în Epoca informației. Deși o mică parte din aceste atacuri au drept rezultat pierderi semnificative și daune, marea majoritate produc pagube mici (care ar echivala cu infracțiuni cum ar fi: încălcarea proprietății private, vandalismul minor sau furturile mici).

A fost estimat că mai mult de 90% dintre aceste atacuri sunt comise folosindu-se mijloace și tehnici disponibile marelui public (incidente raportate de CERT), că doar 1 din 20 de atacuri este observat de victimă, și că doar 1 din 20 este raportat (aceste ultime două statistici sunt rezultatul studiului DISA [„Defensive Information Systems Agency"]. Cote similare au fost raportate și de către alte instituții). Cu toate acestea, se pare că raportarea cotelor ar putea fi în creștere. Îngrijorătoare este prezența unei amenințări „strategice" tehnice.

Mijloacele care există pot cauza daune serioase bunurilor informatice publice și private, proceselor și sistemelor informaționale și pot compromite integritatea informației vitale. Analiștii n-au dificultăți în identificarea grupurilor care au motivații și oportunități pentru a lansa astfel de atacuri. Dată fiind vulnerabilitatea noastră, ca națiune, un RI bine planificat și coordonat poate avea consecințe strategice.

Un astfel de atac, sau amenințarea unui astfel de atac, poate veni în contradicție cu obiectivele politicii noastre externe, poate degrada performanța noastră militară, poate duce la pierderi economice semnificative și chiar la subminarea încrederii cetățenilor noștri în abilitatea guvernului de a-și proteja cetățenii și interesele.

Chiar dacă până acum nu a existat vreun atac care să constituie o astfel de amenințare, simpla existență a mijloacelor prin care se poate duce un astfel de atac, cuplată cu multitudinea motivelor și oportunităților care există, reflectă starea noastră prezentă de vulnerabilitate. Aceste circumstanțe cer acțiuni defensive în interesul publicului. Trebuie să fim mai degrabă „proactivi", decât să reacționăm după o informație de tip „Pearl Harbour". Din ce în ce mai des, un atac strategic reușit va indica calea și îi va încuraja pe alții să plănuiască atacuri similare. De aceea trebuie să ripostăm întărindu-ne latura defensivă.

Fiecare epocă a văzut războiul transformat de tehnologiile și conceptele acelui timp. Epoca informației promite să nu fie diferită din acest punct de vedere, de predecesoarele sale. Unii au denumit războiul din Golf ca fiind primul „Război informațional", alții l-au numit ultimul război din Epoca industrială. Puterea informației a fost clar demonstrată în contextul conflictului tradițional. Informația a îmbunătățit efectiv eficiența tuturor aspectelor războiului, de la logistică, la comandă, control, comunicații, și computere, informații, supraveghere și recunoaștere (C4ISR).

Eficiența SUA și a aliaților săi, în războiul din Golf, a împiedicat cu siguranță adversarii potențiali de a răspunde forțelor noastre într-o manieră pe care Irakul a încercat-o și a stimulat-o. Prin tehnologiile avansate și prin globalizarea economiei, războiul digital oferă posibilitatea unei eficiențe mai mari, devenind astfel o strategie pe care adversarii potențiali se gândesc să o adopte, pentru a îndeplini niște obiective pentru care anterior se căuta o soluționare prin mijloacele războiului tradițional.

Război digital, un subset a ceea ce noi numim RI, implică atacuri care nu sunt fizice asupra informației, proceselor informaționale, și infrastructurii informaționale, care compromite, alterează, produce daune, întrerupe sau distruge informația și/sau întârzie, aduce confuzie, înșeală și blochează procesul informațional și decizional.

Războiul digital posedă câteva dintre caracteristicile pentru

care factorii militari abilitați se luptau în trecut: precizie la un preț scăzut, neparticipare și secret.

Războiul militar amenință capacitatea armată a unei țări de a se interpune între populație și „dușmanii statului", provocând astfel pierderea refugiului. Importanța refugiului poate fi dedusă din dorința noastră de a cheltui importante resurse, în diferite domenii, pentru a asigura cetățenilor noștri un refugiu funcțional în caz de pătrunderi teritoriale.

O altă caracteristică a atacurilor informaționale provine din pierderea refugiului. Atacuri de acest gen, atunci când sunt mai mult decât un incident izolat, creează o percepție a vulnerabilității, a pierderii controlului și a încrederii în capacitatea unui stat de a asigura protecție. Impactul poate să întreacă cu mult pagubele produse.

Această reacție neliniară între daune reale și daune sociale face ca problema războiului digital să fie o provocare specială, deoarece creează o nepotrivire între răspunsurile raționale de apărare și eficiența lor.

Cum răspunde cineva la un set serios de atacuri informaționale? A răspunde cu forțe militare tradiționale poate fi un fapt neacceptat politic sau poate fi ineficace. De cele mai multe ori, nu există un consens privind modul de a trata un astfel de atac, chiar și printre persoanele din domeniul apărării, care sunt preocupate de aceste probleme.

Dată fiind potențiala eficiență a unui război digital ca instrument de putere pentru concurenți și pentru actorii nonstatali, noi, ca societate, trebuie să luăm în serios Epoca informației și noua sa formă de război. Dacă nu o vom face și dacă ne vom baza doar pe arme și concepte de război tradiționale, vom ajunge să construim în secolul XXI propria noastră linie Maginot, care poate fi distrusă cu viteza luminii.

Există persoane care au sugerat că nu suntem, așa cum s-a pretins, atât de vulnerabili la atacurile informaționale, datorită faptului că sistemele noastre dețin un anumit potențial de rezistență

și elasticitate. Acestea au scos în evidență suprapunerile existente la nivelul acestor sisteme și consideră că ar fi foarte greu, pentru oricine, să distrugă complet un set dat de servicii.

Au arătat lipsa de interoperabilitate dintre sistemele moștenite, și spun că ar fi imposibil pentru atacatori să ajungă foarte departe prin pătrunderea chiar și a celor mai slabe sisteme și folosirea lor drept căi de acces pentru a ataca alte sisteme. Ei spun că sistemele noastre și interrelaționările lor sunt dificil de înțeles chiar și pentru noi, deci cu atât mai mult pentru potențialii adversari.

Cu siguranță este o doză mare de adevăr în fiecare argument. Dar această colecție de puncte de vedere are dezavantajele sale. În ce privește considerațiile asupra securității, cinci puncte trebuie subliniate.

· În primul rând, important nu este faptul dacă un atac poate sau nu să distrugă în totalitate un sistem sau un tip de serviciu, ci dacă sunt suficiente daune pentru a atrage atenția și a provoca un comportament de panică, care poate crea la rândul său, o problemă semnificativă, de importanță națională.

În al doilea rând, redundanțele în sisteme sunt numai parțiale și neplanificate. De aceea ele nu sunt nici complete, nici de încredere.

În al treilea rând, sistemele noastre, multe fiind proiectate și construite cu puțină sau chiar fără atenție pentru securitate, sunt dificil de protejat și de securizat.

În al patrulea rând, deoarece nevoile de interconexiune și interoperabilitate cresc, din ce în ce mai multe sisteme sunt legate prin diverse „lucrări auxiliare". Aceste poteci, compromit în multe cazuri, securitatea.

În final, lipsa de securitate produsă de aceste sisteme provoacă renunțarea la cererea de servicii, ceea ce face ca operațiile să fie mai eficiente în multe domenii. Sistemele noastre uzuale au și alte dezavantaje. De exemplu, lipsa interoperabilității duce la risipirea resurselor și la diminuarea eficacității operațiilor. Un lucru trebuie să fie clar: dezavantajele sistemelor noastre nu sunt o

binecuvântare deghizată, ci mai degrabă sursa problemelor care trebuie să fie rezolvate, astfel încât noi să putem profita din plin de oportunitățile pe care tehnologiile informaționale ni le procură.

Primul pas în abordarea oricărei probleme implică dezvoltarea unei *înțelegeri a mediului* („stări ale naturii") cu care avem de-a face, a *opțiunilor* pe care le avem și a *obiectivului* care este căutat. Acest lucru cere o identificare a variabilelor relevante, acelora care pot să influențeze semnificativ rezultatul, dar și subsetul acestor variabile relevante, care sunt controlabile, care formează baza pentru proiectarea operațiunilor.

Într-o problemă atât de complexă ca RI-D, formularea problemei rezolvă trei aspecte. În primul rând, furnizează un schelet util pentru discuție. În al doilea rând, servește să mențină atenția focalizată pe acele arii specifice, care sunt fie necunoscute, fie în dispută. În al treilea rând, servește ca unitate de măsură pentru măsurarea progresului.

În acest caz, *mediul* corespunde naturii amenințării cu care avem de-a face, vis-à-vis de vulnerabilitățile infrastructurii noastre informaționale, în timp ce *opțiunile* noastre corespund strategiilor pe care le adoptăm și acțiunilor pe care le întreprindem pentru a ne apăra pe noi înșine. *Obiectivul* căutat corespunde nivelului performanței infrastructurii, definirea și măsurarea sa fiind o provocare însemnată prin ea însăși și a ei înșiși.

Un punct bun de pornire este încercarea de a dezvolta o înțelegere a naturii amenințării sau mai precis a spectrului amenințărilor relevante. Aceasta presupune o identificare a amenințărilor potențiale și o estimare a probabilității lor. În mod normal, s-ar construi un set de stări ale naturii care sunt reciproc exclusive și colectiv exhaustive, astfel încât o probabilă funcție a densității să poată fi folosită. Stările naturii la care ne referim, corespund amenințărilor potențiale, grupate după un criteriu logic, menit să faciliteze analiza modului în care o strategie de apărare tratează fiecare din aceste amenințări.

Având un concept inițial al naturii și șirul amenințărilor

potențiale, cineva poate să dezvolte strategii de apărare alternative și seturi de acțiuni corespunzătoare, pentru a le opune uneia sau mai multor amenințări. Depinde mult, însă de ce variabile credem noi că putem sau că ar trebui să controlăm.

Fiecare strategie de apărare, cu setul său corespunzător de acțiuni, trebuie apoi să fie analizată în funcție de fiecare amenințare. Rezultatele acestor analize vor fi o caracterizare a rezultatelor sau a efectelor obținute prin urmărirea fiecărei strategii de apărare care să țină cont de fiecare amenințare.

Aceste efecte, care sunt în principal descrieri ale rezultatelor (de exemplu: numărul penetrărilor și consecințele lor), trebuie apoi să fie traduse în măsuri de valoare, măsuri care reprezintă impactul lor. Costurile și beneficiile asigura o bază rațională pentru realizarea unei strategii de apărare corespunzătoare. Datorită rolului central pe care tipologia amenințărilor îl joacă în formularea problemei, ne vom întoarce atenția acum, asupra examinării acestor categorii de amenințări.

O înfățișare grafică a topologiei amenințării este prezentată în Figura 2. Natura neregulată a spațiului indică faptul că granițele sale nu sunt bine definite. Cu toate acestea, amenințările se pot grupa după criteriul gravității consecințelor lor (de la stânga la dreapta). Consecințele asociate unui eșec merg de la consecințe limitate și izolate, la consecințe de proporții catastrofice.

Într-o serie de imagini, de la Figura 3 până la Figura 6, sunt înfățișate diferite aspecte ale topologiei amenințării. În Figura 3, spațiul amenințării este împărțit în trei zone. În partea din stânga a spațiului putem să grupăm marea majoritate a amenințărilor, a **amenințărilor de fiecare zi**. Aceste **amenințări de fiecare zi** („Everyday Threats"), au un anumit cost, însă nu amenință securitatea noastră națională. În partea din dreapta a spectrului amenințării este o mică suprafață care reprezintă acele **amenințări strategice** care au implicații asupra securității naționale. A treia zonă conține amenințări care pot avea implicații asupra securității naționale. Aceste **amenințări potențial strategice** („Potentially Strategic Threats") reprezintă o provocare dificilă, aparte.

Există un număr relativ mic de amenințări, cu care marea majoritate ar fi de acord că au implicații strategice (Figura 4), care trebuie apărate cu multă vigoare. Atacurile împotriva sistemelor care controlează armele de distrugere în masă („WMD") sau asupra rețelei noastre de comunicații urgente („MEECN") aparțin clar acestei categorii.

Alte ținte strategice sunt sistemele de informare și comunicare, asociate cu Autoritatea națională de comandă („National Command Authority"), câteva dintre sistemele noastre de comandă, control, comunicare și informații (C31) și câteva dintre sistemele noastre de informații, mai ales informațiile care privesc sursele și metodele. În afară de aceste seturi de amenințări, care aparțin clar fie categoriilor **amenințări de fiecare zi**, fie categoriilor **amenințări strategice**, sunt și alte clase de amenințări, care lărgesc spectrul amenințărilor.

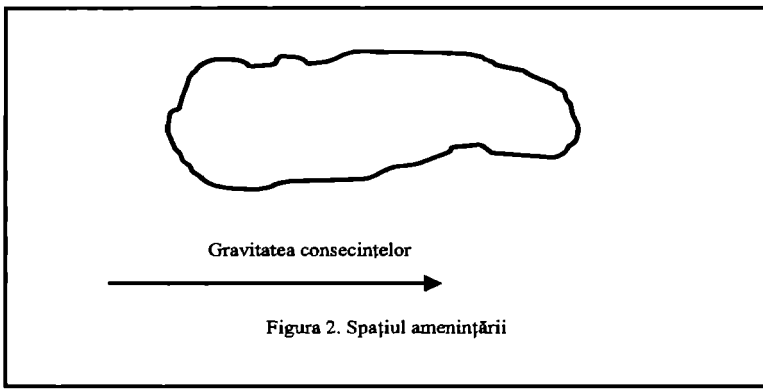


Figura 2. Spațiul amenințării

Atacurile asupra infrastructurii noastre naționale (Figura 5) nu aparțin clar unei singure zone a tipologiei amenințărilor, ci tuturor celor trei clase de amenințări. Aceste atacuri, asupra siguranței publice, sistemelor și serviciilor de distribuire a energiei, asupra sistemelor și serviciilor financiare și de comunicații au implicații diferite și consecințe care depind de natura specifică și de circumstanțele în care se desfășoară atacul.

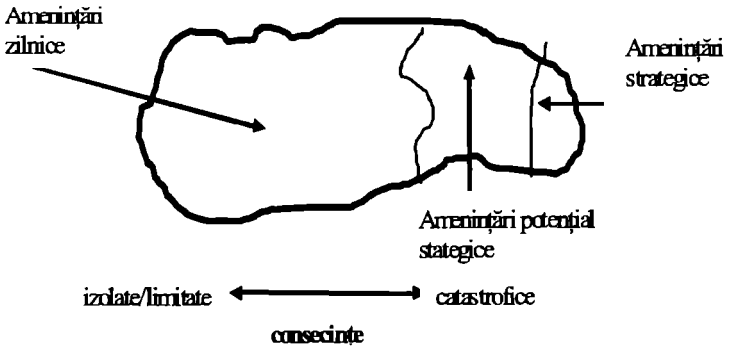
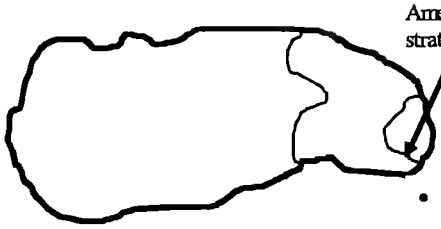


Figura 3. Zonele spațiului amenințării



- WMD / MEECN
- NCA
- Câteva C3I
- Intelligence
- Surse / Metode

Figura 4. Amenințări strategice

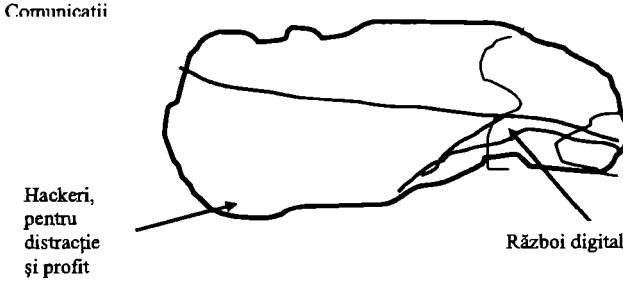


Figura 5. Infrastructura amenințărilor

În timp ce unele dintre aceste atacuri pot avea consecințe serioase, sub forma unor pierderi semnificative de date, servicii întrerupte sau bunuri și servicii furate, numai un mic număr dintre aceste atacuri izolate poate avea consecințe potențial strategice.

Cu toate acestea, atacurile asupra infrastructurii pot fi serioase, dacă sunt bine planificate și bine coordonate. Pentru aceasta este nevoie de un adversar cu un scop bine definit, cu un sistem sofisticat și cu o bună organizare. Acestui tip de atac i se potrivește denumirea de **război digital** („Digital Warfare"). În funcție de nivelul de sofisticare al unui atac, consecințele acestuia pot ajunge până la consecințe strategice.

Un punct important, care trebuie subliniat, este cel al naturii haotice a atacurilor asupra infrastructurii. Comportamentul haotic presupune o relație neliniară între input și output, unde predicția devine extrem de dificilă, dacă nu imposibilă. Două scenarii ilustrează această natura haotică.

În primul caz, un atac asupra infrastructurii poate să provoace o serie de consecințe apropiate, dificil de prezis și care măresc cu mult efectele atacului.

În al doilea caz, o serie de atacuri pot da dovadă de un comportament haotic atunci când suma consecințelor lor nu poate fi determinată prin adăugarea consecințelor lor individuale, sau când efectul lor cumulat întrece de departe suma efectelor individuale, a unei serii de întâmplări independente.

Aceste două scenarii nu sunt modele neobișnuite. Aceste modele se regăsesc și în natură dând naștere unor discipline științifice, cum ar fi cele ale complexității, ale catastrofei, și teoria complexității.

La fel stau lucrurile și în privința atacurilor asupra țintelor comerciale, reprezentate în Figura 6. În categoria amenințărilor de zi cu zi intră atacuri care, în Epoca informației, sunt o versiune a fraudei și furtului - o continuare a crimei gulerelor albe și o transformare a unei crime mai violente într-o formă care nu e fizică.

Așa cum a arătat Dr. Horton (PDSAD (C31)), când unul dintre cei mai celebri hoți de bănci a fost întrebat de ce jefuiește bănci (dat fiind faptul că ele sunt așa de bine apărate), acesta a remarcat: „acolo sunt banii". Ei bine, „digital money" (bunurile și serviciile) reprezintă banii în Epoca informației.

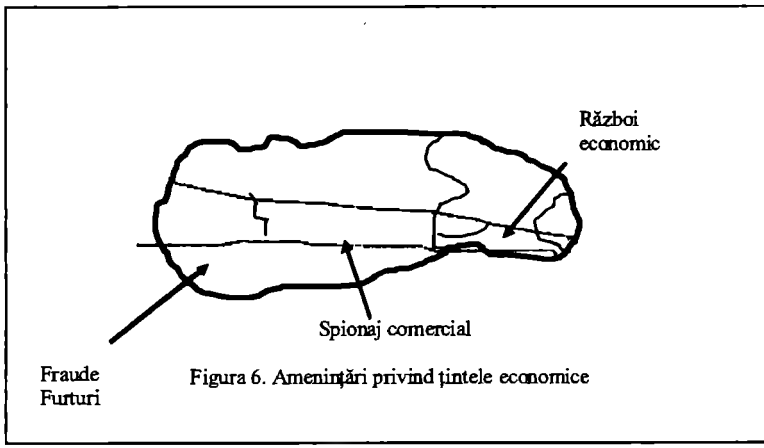


Figura 6. Amenințări privind țintele economice

Ca și atacurile asupra infrastructurii, atacurile asupra țintelor comerciale se pot manifesta în funcție de circumstanțe, de la amenințări de fiecare zi până la amenințări strategice. Atacurile asupra țintelor comerciale, realizate de către diferite organizații, nu vizează, de obicei, în mod direct banii, ci mai degrabă informații vitale (ex. secrete comerciale) și au un mare potențial de a provoca efecte mai serioase decât furturile izolate. Aceste atacuri, sub forma spionajului comercial, au consecințe potențial strategice, mai ales atunci când sunt vizate ramuri industriale cheie, de către companii străine.

Spionajul comercial se transformă în război economic, care ar putea să aibă consecințe strategice, atunci când există eforturi dirijate de state, de organizații internaționale, sau de alte grupuri străine.

Așa cum se poate vedea din seria de înfățișări grafice ale tipologiei amenințării prezentate mai sus, amenințarea este multidimensională, într-un fel dezordonată chiar, și se poate comporta într-o manieră haotică. Natura dinamică și interactivă a amenințării face apărarea împotriva atacurilor să fie mai dificilă.

Atacatorii și apărătorii sunt prinși într-o bătălie continuă a inteligențelor și resurselor (Figura 7). Din păcate, atacanții posedă câteva avantaje. De exemplu, atacatorul poate să aleagă timpul, locul, mijloacele și metoda de atac. Latura tehnologică este tot de partea atacatorului, deoarece este foarte dificil să dezvolți apărări perfecte la un preț pe care să ți-l permiți. De aceea, vor exista întotdeauna „găuri".

Care dintre acestea vor fi exploatate rămâne o necunoscută până în momentul atacului. Din acest motiv, atacul este, de obicei, cu un pas înaintea apărării. Atacatorii au, de asemenea, avantajul de a putea controla atacul, mult mai ușor decât ar putea s-o facă cei atacați.

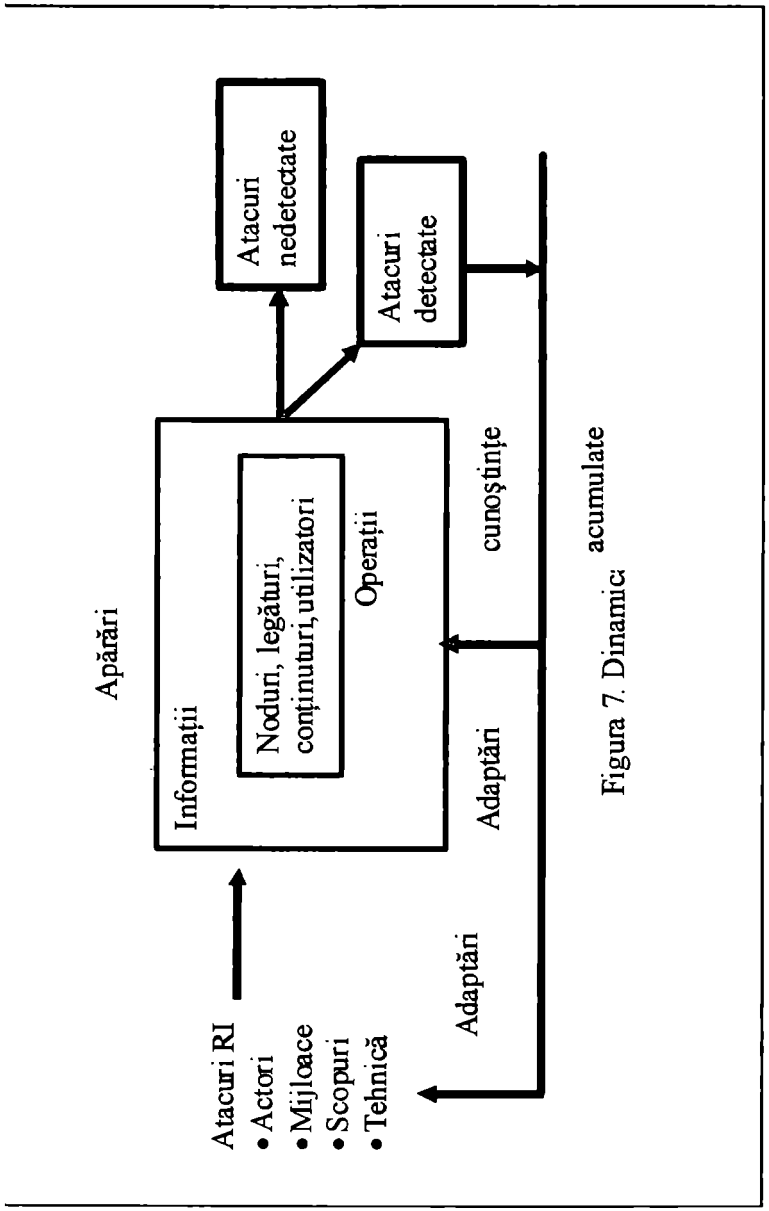


Figura 7. Dinamica

Orice întâmplare este un mediu de studiu pentru atacatori și apărători – este un mediu dinamic. În acest mediu organic, atacatorii învață din atacurile nedetectate în momentul desfășurării lor, indiferent dacă au fost reușite sau nu. Atât atacatorii cât și apărătorii se perfecționează și jocul continuă.

Acest aspect al amenințării indică faptul că apărarea trebuie să constituie o preocupare continuă. De asemenea, sugerează faptul că strângerea și analizarea informațiilor despre atacuri este vitală pentru a putea ține pasul cu atacatorii. În concluzie, apărătorii trebuie să fie activi și să-și asume eforturi care să conducă la o anticipare a metodelor atacului, astfel încât să poată fi dezvoltată o apărare eficace.

Problema privind eficacitatea unei apărări în fața unei varietăți de atacuri potențiale este exacerbată de: incapacitatea noastră de a dezvolta o relație simplă, între un tip de atac sau amenințare și o organizare, de relația esențială, neliniară, dintre rezultat și valoare și de faptul că variabilele-cheie nu sunt sub controlul nostru.

Descompunerea unei probleme ne ajută, uneori, să facem progrese, ușurând, cel puțin, stabilirea responsabilităților la nivelul instituțiilor. Așa cum am văzut, problema RI-D rezistă descompunerii de-a lungul liniei organizaționale. Aceasta se întâmplă deoarece există o slabă cartografiere a relației dintre amenințare și organizare, din două puncte de vedere.

În primul rând, ținta organizațională a atacului este foarte puțin legată de topologia amenințării, deoarece atacul unei anumite organizații, poate avea drept rezultat un set de consecințe, care lărgesc spectrul amenințărilor.

În al doilea rând, nu există o delimitare clară între responsabilitatea organizațională și topologia amenințării. Acest lucru este mai ales adevărat atunci când vorbim de suprafața identificată ca fiind potențial strategică.

Este întotdeauna mai ușor să rezolvi probleme cu funcții obiective predictibile sau cu măsuri ale valorii. Așa cum am văzut, în RI-D există situații în care relațiile dintre evenimente și variabile

se comportă într-o manieră haotică. Acest lucru introduce în ecuație o doză mare de incertitudine.

Dacă aceste două caracteristici ale problemei RI-D nu prezintă provocări semnificative, ne confruntăm totuși cu faptul că unele dintre variabilele-cheie, care au influență asupra rezultatelor și valorilor acestor rezultate, sunt numai parțial controlabile. De exemplu, fiecare dintre următoarele variabile, dacă este pe deplin controlabilă, ar putea fie să reducă semnificativ numărul sau severitatea atacurilor, fie să reducă impactul atacurilor: proliferarea tehnologiei, nivelul de conștientizare și pregătire a personalului, disponibilitatea expertizei pe computer, sistemul de apărare și percepțiile publicului.

Am ajuns la sfârșitul discuției despre *natura* și *caracteristicile* RI-D. În continuare este prezentat și discutat un posibil mod de soluționare a problemei.

Soluția propusă în acest material este cea a unei strategii de „*apărare în adâncime*", strategie care implică o succesiune de bariere defensive, din ce în ce mai puternice sau „mai înalte", ce acționează împreună, pentru a descompune spectrul amenințărilor la componentele manageriale. În continuare, vom detalia această strategie a RI-D, natura separării responsabilităților, unele din condițiile obligatorii pentru realizarea unui progres, provocările-cheie care apar, respectiv elementele unui plan de acțiune pentru organizațiile cu responsabilități în domeniul RI-D.

Strategia de „apărare în adâncime" propusă, prezentată în Figura 8, constă în trei linii de apărare. Fiecare linie de apărare este proiectată în așa fel încât să ia în considerare amenințările asociate cu o anumită zonă a tipologiei amenințării.

Prima linie de apărare este apărarea împotriva **atacurilor zilnice**, care constituie partea cea mai consistentă a tipologiei de amenințare. Pe baza informației disponibile, marea majoritate a acestor atacuri pot fi respinse cu apărări de bază.

Cele mai înalte niveluri de apărare, asociate **atacurilor potențial strategice** sau **strategice** sunt responsabile cu împiedicarea celor mai sofisticate atacuri, care, însă, sunt și cele mai rare.

- Abordarea apărării în adâncime
- Majoritatea atacurilor pot fi respinse cu apărări de bază
- Niveluri mai înalte ale apărării sunt responsabile cu împiedicarea celor mai sofisticate atacuri, care sunt însă şi cele mai puţine, din mai puţine surse posibile
- Combinarea filozofiilor „mai întâi informaţia" şi „mai întâi securitatea"

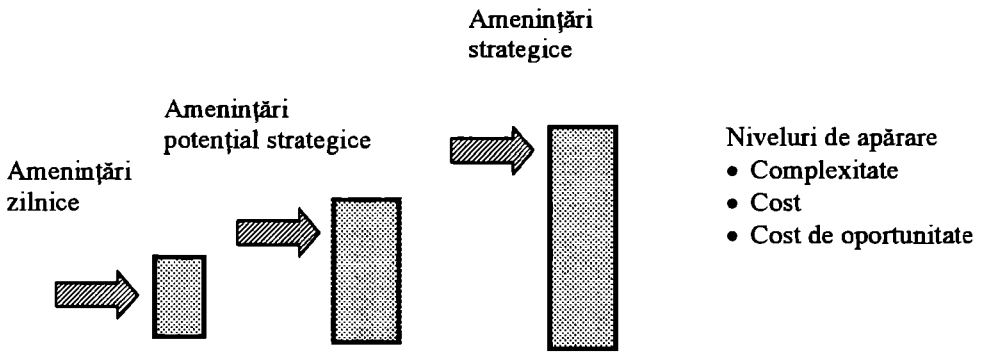


Fig. 8 Strategia de „apărare în adâncime"

De exemplu, atacurile cu implicații strategice ar trebui să treacă de primele două linii de apărare, care ar trebui să filtreze toate atacurile, exceptând doar adversarii cei mai pricepuți, cei mai persistenți, cu cele mai bune și mai performante resurse. Acesta înseamnă că am putea să ne concentrăm eforturile asupra monitorizării unui segment mai redus al populației, fapt ce va spori șansele de a obține în apărare succesul scontat.

Strategia defensivă înseamnă, de asemenea, posibilitatea de a aplica diferite abordări filozofice fiecărei linii de apărare, în funcție de natura amenințării. Cele două puncte de vedere ale spectrului filosofic pot fi acceptate ca abordări intitulate „mai întâi informația", respectiv „mai întâi securitatea".

În zona zilnică a tipologiei de amenințare, abordarea noastră a pus accent pe accesul la informație. În zona strategică, se pune accent în primul rând pe securitate, prin restricționarea accesului și a conexiunii.

Figura 9 reprezintă grafic o separare a responsabilității primare pentru RI-D, între sectorul public și cel privat, ca o funcție a tipologiei de amenințare. Termenul „primar" este utilizat pentru a sublinia faptul că, atât instituțiile publice cât și cele private au responsabilități în privința RI-D, chiar dacă acestea sunt asociate, într-un anumit domeniu, unuia din sectoarele public sau privat.

Zonele tipologice asociate amenințărilor zilnice sau strategice sunt cele mai evidente. Responsabilitatea primară pentru amenințarea zilnică ar trebui să revină sectorului privat. Rezolvarea acestei amenințări reprezintă costul de a face afaceri în Era informației. Presupunând costul relativ scăzut al apărării împotriva acestor tipuri de amenințări, atribuirea acestei responsabilități sectorului privat devine posibilă. Mai mult, organizațiile private sunt evident în cea mai bună poziție pentru a înțelege propriile sisteme informaționale și nevoile și preocupările clienților lor.

Răspunsul la amenințările strategice este evident sarcina sectorului public, deși o apărare adecvată va implica unele coordonări cu sectorul privat și cu organizațiile internaționale, în special când apărarea este construită pentru a face față amenințărilor asupra infrastructurii informaționale naționale sau asupra altor instituții ce furnizează servicii vitale.

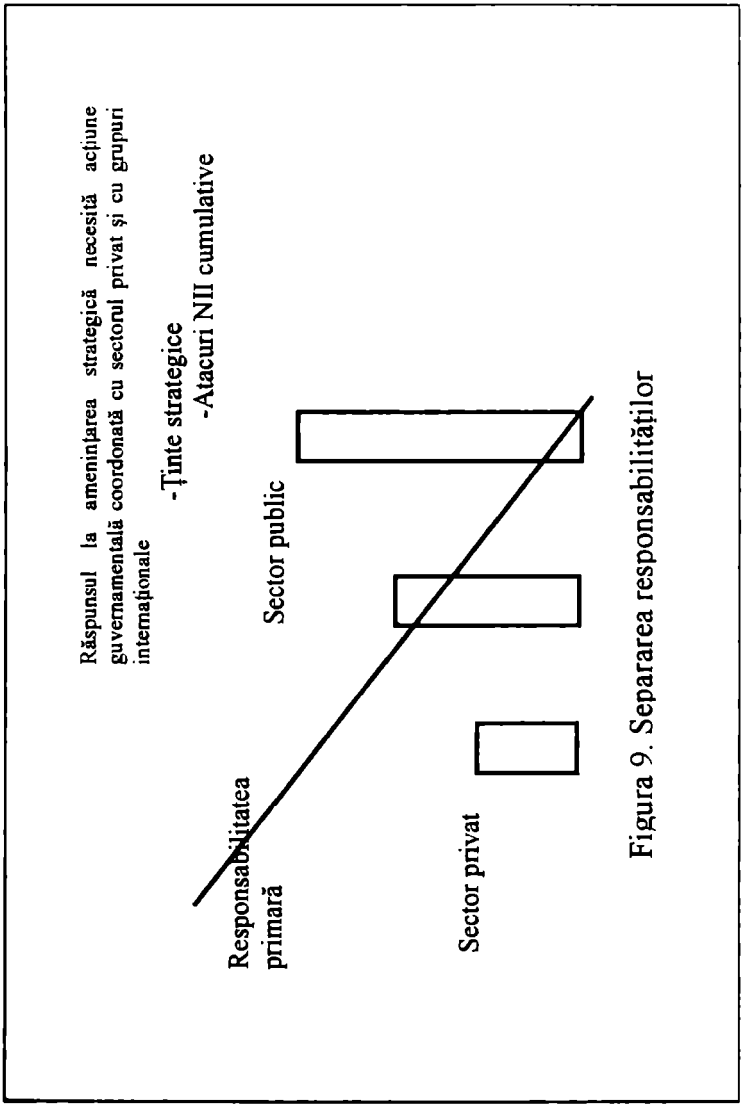

Răspunsul la amenințarea strategică necesită acțiune guvernamentală coordonată cu sectorul privat și cu grupuri internaționale
-Ținte strategice
-Atacuri NII cumulative
Sector public
Responsabilitatea primară
Sector privat

Figura 9. Separarea responsabilităților

Amenințarea zilnică poate fi și ar trebui să fie respinsă de fiecare instituție
-Costul de a face afaceri în era informației
-Există soluții la cost scăzut pentru majoritatea amenințărilor
-Instituțiile sunt în cea mai bună postură pentru a înțelege sistemele /clienții

Este mai puțin evidentă posibilitatea stabilirii responsabilității primare de apărare împotriva amenințărilor din zonele potențial strategice ale topologiei de amenințare. Această zonă ar putea fi numită „zonă de colaborare", unde este nevoie ca sectorul public și cel privat să conlucreze pentru a înțelege amenințarea și pentru a dezvolta mecanisme eficiente care să țină cont de ea.

Eforturile pentru a realiza o colaborare efectivă vor necesita depășirea perspectivelor diferite de înțelegere ale instituțiilor. Instituțiile comerciale tradiționale tratează atacurile zilnice ca un simplu cost necesar pentru a face afaceri, ce nu diferă semnificativ de un furt. Contramăsurile luate au o valoare așteptată definită și sunt angajate când costul lor efectiv este mai mic decât valoarea lor așteptată.

Instituțiile tradiționale din sectorul privat răspund la evenimente de probabilitate relativ redusă cu costuri posibil mai mari, rezultate din cumpărarea de asigurări sau obținute prin furnizarea unei asigurări proprii.

Perspectiva securității informației, oferită de instituțiile ce operează cu informații și sisteme considerate vitale pentru securitatea noastră națională, este destul de diferită. Spre deosebire de numeroasele atacuri informaționale asupra sistemelelor din sectorul privat, costul unei breșe în securitatea unor informații de importanță națională nu poate fi ușor determinat. Evidențierea costului actual, al unui incident specific, este datorat faptului potrivit căruia protecția sporită a integrității unor informații de securitate națională și a sistemelor ce le vehiculează are o valoare intrinsecă înglobată. Riscul evitării este răspunsul adoptat în aceste situații.

Potrivit naturii tipologiei de amenințare a RI, securitatea informațiilor din sectorul național și sectorul privat sunt strâns legate. Atacurile asupra infrastructurii informaționale globale sau naționale pot afecta serios organizațiile din sectorul privat. Același lucru se întâmplă și în cazul atacurilor asupra instituțiilor-cheie din sectorul privat, ce pot furniza servicii vitale, atacuri care au implicații serioase în privința securității naționale.

Aceste situații sunt conținute în zona potențial strategică a topologiei de amenințare. Se propune ca în această zonă, spre deosebire de **abordarea** simplă **„dolari și cenți"**, specifică zonei zilnice a tipologiei de amenințare sau **abordării prin evitarea riscului**, specifică zonei strategice a tipologiei de amenințare, să se adopte o **abordare de management al riscului** colectiv. Acesta este evident un domeniu care necesită ca apărările să fie coordonate îndeaproape.

Urmând firul logic a ceea ce am prezentat în legătură cu natura acestei probleme, ar trebui să fie evident pentru oricine că orice încercare de a realiza gestionarea RI-D într-o abordare centralizată este sortită eșecului. Dacă cineva are vreo îndoială, ar trebui să-și reamintească de amenințarea slabă existentă la cartografierea organizațională, care previne rezolvarea efectivă a problemei cu „lanțuri de comandă pure" și limitele posibilității Guvernului sau ale unei alte instituții, de a controla variabile relevante.

Potrivit urgenței și importanței acestei probleme este necesară o viziune pro-activă. Totuși ar trebui să fie evident că o abordare de tip „laissez-faire" (rezolvare de la sine) este de asemenea sortită eșecului.

Este necesară o formă de orchestrație (sincronizare) colectivă pentru a dezvolta gradul de conștientizare (luare în considerare) și înțelegere a amenințării pentru a dezvolta, în consecință, apărările necesare. Guvernul trebuie să stabilească ceea ce eu am numit „cadru pentru progres".

Rolurile și responsabilitățile specifice sectorului public și privat vor fi diferite, în funcție de tipul de amenințări pe care le-am evidențiat în scurta noastră trecere în revistă a fiecărei din cele trei zone importante ale tipologiei de amenințare. În timp ce această discuție s-a focalizat pe rolurile, responsabilitățile și nevoia de colaborare dintre structurile specifice SUA, problema RI-D a depășit granițele naționale. Fără acorduri internaționale specifice și cooperare între națiuni și organizații internaționale, posibilitatea noastră colectivă de a gestiona amenințările va fi minimă.

Dezvoltarea celor șase domenii identificate în grafic vor netezi considerabil drumul nostru și ne vor accelera progresul.

În primul rând, una din condițiile obligatorii pentru progres este luarea în considerare a problemei și a complexităților ei, precum și generarea unui climat ce va facilita discuția și cooperarea între multe grupuri și organizații, care trebuie să fie parte a acestui efort. Potrivit evenimentelor recente privind unele aspecte de securitate a informațiilor, avem nevoie să începem reconstruirea legăturilor dintre unele grupuri și organizații din sectorul public și privat.

În al doilea rând, este important să ne desfășurăm activitatea potrivit unei viziuni bine definite, care să evidențieze clar ce încercăm să realizăm și rolul corespunzător Guvernului.

În al treilea rând, „regulile jocului" trebuie dezvoltate și promulgate. Multe din legile și regulamentele noastre curente nu iau în considerare realitățile Erei informației. Un set de reguli trebuie să se refere la stabilirea standardelor de securitate informațională sau la un nivel minim de apărare ce trebuie asociat cu diferite tipuri de date și servicii informaționale. Acestea vor fi similare cu recentele standarde private.

În al patrulea rând, interesul propriu, chiar lămurirea interesului propriu și dorința indivizilor și organizațiilor de a fi buni cetățeni, nu sunt suficiente pentru a ne asigura că vor fi dezvoltate și angajate acțiunile și apărările cele mai potrivite. Trebuie furnizate organizațiilor guvernamentale resursele necesare pentru a ajuta la implementarea acestui cadru pentru progres și la implementarea apărărilor necesare. E nevoie, de asemenea, să oferim stimulente care să încurajeze organizațiile din sectorul public. În anumite cazuri particulare, Guvernul va fi nevoit chiar să furnizeze fonduri organizațiilor din sectorul privat, pentru a pune la punct un sistem de securitate eficient.

În al cincilea rând, soluția la această problemă depinde în mare măsură de cooperarea dintre organizații și grupuri distincte. Este nevoie de dezvoltarea mecanismelor capabile să faciliteze și

să sporească cooperarea (incluzând stabilirea conținutului colaborării, a grupurilor și a locurilor special destinate).

În al șaselea rând, avem nevoie să stabilim responsabilitatea pentru numărul mare de sarcini pe care le implică un RI-D. Avem nevoie să decidem chestiuni de jurisdicție. Avem nevoie să delimităm obligațiile și le facem cunoscute. În final, este necesar să stabilim clar responsabilitatea fiecărei organizații. Natura responsabilităților organizaționale este discutată detaliat în continuare.

Nici unul din cele șase aspecte ale cadrului pentru progres nu încurajează ideea punerii în practică prea curând a acestuia. Considerând numai nevoia de revizuire a procesului legislativ, putem observa că va mai dura câtva timp înainte ca acești stâlpi de fundamentare să fie la locul lor. Totuși e necesar să începem deja să purtăm o discuție despre aceste elemente și să încercăm să ținem atenția focalizată pe acest subiect.

Responsabilitățile organizațiilor din sectorul public și privat diferă în funcție de zona de amenințare. În fiecare zonă de amenințare, de la cea zilnică la cea strategică, fiecare sector al societății are unele responsabilități.

Responsabilități privind amenințările zilnice.

Responsabilitatea primară pentru zona zilnică a tipologiei de amenințare revine sectorului privat. În primul rând, organizațiile din sectorul privat trebuie să-și asume responsabilitatea pentru protecția propriilor lor sisteme. Când legile și regulamentele de securitate vor fi formulate și adoptate, aceste organizații vor fi de asemenea responsabile pentru aderarea la aceste reguli ale jocului.

Dat fiind timpul necesar pentru dezvoltarea și punerea în funcțiune a unui cadru legal și regulamentar pentru operarea cu numărul mare de elemente ale securității informaționale, se propune ca pe bază voluntară, organizațiile din sectorul privat să-și asume responsabilitatea pentru raportarea incidentelor. Este necesar să subliniem importanța culegerii și analizei de informații referitoare la atacurile informaționale. Fără dezvoltarea unui

ansamblu de cunoștințe referitoare la aceste atacuri, eforturile pentru construirea apărărilor vor fi semnificativ îngreunate

Guvernul (incluzând nivelul federal, statal și local) trebuie să-și asume responsabilități certe pentru această regiune a tipologiei de amenințare. În mod evident, Guvernul poartă responsabilitatea pentru protecția sistemelor proprii și pentru impunerea legilor și regulamentelor corespunzătoare. Dată fiind importanța realizării colaborării internaționale în privința acestei probleme, ce nu cunoaște granițe statale, Guvernul trebuie să realizeze negocierea tratatelor și acordurilor necesare.

Evident, culegerea datelor despre propriile sisteme este, de asemenea, responsabilitatea Guvernului. Dată fiind importanța schimbului de informații, necesară obținerii unei imagini precise a situației, Guvernul trebuie să stabilească mecanisme pentru distribuirea, analiza datelor și furnizarea rezultatelor. Vor trebui abordate elemente referitoare la clasificarea și securitatea datelor. Trebuie găsită o soluție pentru a obține informațiile de care organizațiile și indivizii au nevoie pentru a se putea apăra ei înșiși.

Guvernul federal are responsabilitatea pentru apărare în zona strategică a tipologiei de amenințare, utilizând suport din partea sectorului privat și a guvernelor locale. Dată fiind dinamica și natura interactivă a acestei situații, este important ca amenințarea să fie înțeleasă cât mai bine. Cu toate acestea, utilizând informația culeasă precum și informația raportată de alții, Guvernul federal are responsabilitatea analizei strategice.

Guvernul federal are nevoie, de asemenea, să dezvolte o strategie de descurajare a potențialilor atacatori. Sistemele strategice trebuie să fie monitorizate și trebuie elaborate operații de supraveghere.

Evident, Guvernul federal are responsabilitatea protejării informației strategice și a sistemelor ce colectează, stochează, prelucrează și transmit aceste informații.

În final, Guvernul federal trebuie să dezvolte planuri pentru reconstrucția sistemelor avariate sau distruse și a informațiilor

pierdute sau compromise, dar pentru elaborarea celor mai eficiente planuri ar trebui simulată o astfel de situație.

Sectorul privat are, de asemenea, un rol de jucat în această zonă a tiopologiei de amenințare. Mai întâi, multe sisteme strategice depind, într-o anumită măsură, de disponibilitatea și integritatea sistemului privat sau de informațiile din sistemele guvernamentale de stat și locale. În al doilea rând, unele sectoare private sau unele sisteme informaționale guvernamentale locale și de stat pot fi atât de importante încât au, indiferent de intențiile și scopurile atacatorilor, un caracter strategic. În cele două cazuri, organizațiile trebuie să coopereze cu Guvernul federal pentru a proteja aceste sisteme informaționale. Dezvoltarea unei înțelegeri adecvate a amenințării necesită ca toate organizațiile să raporteze incidente și să partajeze datele referitoare la atacurile care au avut loc. Astfel, altă responsabilitate ce trebuie să fie asumată de organizațiile din sectorul privat este promptitudinea raportării incidentelor.

Separarea responsabilităților pentru această zonă a tipologiei de amenințare nu este atât de ușor de realizat ca pentru celelalte două zone. În această zonă de colaborare, organizațiile din sectorul public și privat trebuie să găsească căi și să creeze mecanisme ce generează o percepție distribuită asupra naturii amenințării, în particular asupra acelor aspecte ale situației ce sporesc probabilitatea consecințelor strategice. Suplimentar, ar trebui să fie găsite modalități pentru a întări apărarea noastră, prin posibilitatea de a diminua efectele atacurilor în această zonă și chiar de a le împiedica să aibă consecințe strategice.

În această zonă e necesar ca Guvernul să colaboreze pentru dezvoltarea înțelegerii amenințării, în timp ce sectorul privat trebuie să sprijine eforturile Guvernului prin furnizarea datelor incidente. De asemenea, Guvernul trebuie să aibă inițiativa în dezvoltarea coordonării mecanismelor proiectate, să sprijine atât îmbunătățirea înțelegerii cât și coordonarea apărărilor.

Cele două mari provocări asociate acestei zone de amenințare

sunt, mai întâi, identificarea începutului unui atac cu semnificație strategică, caracterizarea naturii și scopului atacului și în al doilea rând, efectuarea tranziției de la „starea de pace" la „starea de război". Succesul proceselor și mecanismelor dezvoltate prin coordonarea acestei tranziții va fi important pentru succesul oricărei strategii a RI-D. Acest lucru include nu numai îmbunătățirea tehnicilor și instrumentelor de detectare, dar și îmbunătățirea posibilității de a stăpâni un atac, și în felul acesta de a limita extinderea pagubelor și consecințelor sale. E nevoie ca Guvernul să asiste sectorul privat în aceste eforturi prin furnizarea resurselor și suportului tehnic. Resursele pot lua forma unor taxe-stimulent (de încurajare) sau a unor plăți directe, în cazul unor sisteme din sectorul privat considerate a fi de importanță strategică.

Pentru oricine care prosperă din provocări, apărarea împotriva RI este o zonă de muncă importantă. Există cinci provocări cheie cu care avem de-a face.

Prima provocare implică dezvoltarea unei mai bune înțelegeri a naturii și caracteristicilor amenințării, în societate și între instituțiile acesteia. Succesul implică ca fiecare să fie familiarizat cu caracteristicile amenințării. Totuși este important ca noi să continuăm să muncim pentru a spori considerarea acestei probleme și a dezvolta o mai bună înțelegere, atât a naturii amenințării cât și a vulnerabilității noastre.

A doua provocare o reprezintă dezvoltarea unei strategii de ripostă a atacurilor informaționale digitale. Prima regulă a apărării este riposta. Nu este alocat suficient efort pentru dezvoltarea și aplicarea strategiilor posibile. ACTIS a sponsorizat un atelier de lucru pe acest subiect. Acest atelier a fost un mare succes, oferindu-le participanților o mai bună idee despre cele mai recente reflecții pe acest subiect, stimulând interesul pentru subiect și aducând în atenție unele elemente cheie (lucrările acestui atelier au fost publicate și sunt disponibile prin intermediul ACTIS).

A treia și a patra provocare implică dezvoltarea mijloacelor de furnizare a avertizării pentru atacuri și modalități de apărare de succes. Îmbunătățirea posibilității noastre de a identifica existența unui atac și de a furniza indicații și avertismente despre atacuri într-un anumită perioadă în timp, este poate cea mai dificilă provocare cu care avem de-a face.

Dezvoltarea unui mod de indicare și avertisment presupune nu numai posibilități de atac tactic și strategic, dar și posibilitatea de a ști că un atac a început și de a stabili, cu o anumită marjă de incertitudine, scopul acestuia. Ținând cont de faptul că, în mod curent, un atac în desfășurare nu este sesizat, această provocare capătă o semnificație importantă.

Nu este numai o provocare tehnică, ci și una organizațională (așa cum am menționat mai devreme). Informațiile necesare pentru a furniza avertizarea despre o acțiune iminentă și un atac în stadiile lui timpurii este cel mai bine să vină din partea organizațiilor sectorului privat, ale căror structuri de raportare ar trebui să pună la dispoziție, într-un timp scurt, toate datele relevante.

Astfel, un atac de semnificație strategică poate să se fi încheiat înainte ca noi să realizăm existența lui și să fim în măsură să trecem la „starea de război", lucru ce determină sporirea cerințelor de raportare și coordonarea necesară pentru a aprecia situația și a răspunde corespunzător.

Ca rezultat al participării mele la o serie de jocuri de tip „după o zi" („day after") dezvoltate de RAND pentru ASD (C3I), am ajuns la concluzia că nu vom fi în măsură să răspundem la timp, la astfel de atacuri, decât dacă există:

1) înțelegere și luare în considerare a naturii posibilităților războiului strategic și a propriilor noastre vulnerabilități, nu numai printre oficialitățile-cheie din organizațiile publice și private, dar și din Congres, din cadrul mass-mediei și a publicului;

2) o mai bună înțelegere a arsenalului ofensiv aflat la dispoziția noastră, în special a efectelor directe, indirecte și colaterale pe care acesta le poate cauza;

3) un sistem de preacord pentru alertă, similar cu sistemul DEFCON, ale cărui nivele susțin cunoașterea și înțelegerea proceselor și acțiunilor practicate;

4) un proces de apreciere a pagubelor corespunzătoare RI.

Construirea unui sistem de tip DEFCON pentru RI-D va necesita investirea unei cantități considerabile de capital intelectual, precum și o bună coordonare între Congres și numărul mare de agenții și departamente guvernamentale, asociații industriale și organizații private.

Opțiunile bine gândite, ce se adresează atât nevoii de culegere de informații și de realizare a unei analize aprofundate, cât și nevoii de a lua măsuri de prevenire sau de control al pagubelor, sunt esențiale pentru considerarea acestei amenințări. Dată fiind topologia amenințării, împărțită în trei zone, și natura foarte diferită a fiecăreia, implementarea strategiei de „apărare în adâncime" va fi o întreprindere considerabilă.

A cincia provocare se referă la dezvoltarea răspunsurilor corespunzătoare unor astfel de atacuri. Răspunsurile date acestor atacuri includ identificarea, interdicția, previziunea și pedepsirea (și chiar răzbunarea).

Avem mult de învățat și pe mulți de educat. Pentru a conștientiza amenințările și consecințele unui RI nu este suficientă numai citirea romanelor sau mersul la filme. Când singurul contact cu subiectul este prin ficțiune nu este nici o mirare că amenințarea poate fi tratată ca fiind ficțiune. Există încă mulți indivizi ocupând poziții-cheie atât în sectorul public cât și în sectorul privat, care au nevoie să înțeleagă mai bine aceste probleme, pentru a fi mai motivați în abordarea fenomenelor.

Pe de altă parte, recunoaștem că nu posedăm o abundentă informație factuală.

Ignoranța noastră în privința naturii atacurilor potențiale este oglindită de lipsa de cunoștințe despre eficacitatea tehnicilor și strategiilor defensive dezvoltate în prezent.

Când sistemele noastre nu sunt monitorizate adecvat și

incidentele nu sunt înregistrate și investigate corect, este greu de apreciat cum am putea dezvolta înțelegerea profundă atât a amenințării cât și a eficacității apărării necesare. Intensificarea culegerii de informații și a analizei aplicate este necesară pentru a furniza fundamentarea empirică pentru:

a) sporirea conștientizării (luării în considerare);
b) sporirea înțelegerii noastre;
c) planificarea sprijinului;
d) dezvoltarea apărărilor efective.

Date fiind limitările pe care le avem impuse în cadrul unei colectări de informații interne, este puțin probabil că vor fi colectate și analizate de către Guvern informații suficiente pentru a determina natura și amploarea unui atac informațional, în stadiile lui timpurii.

Totuși, este extrem de important ca atunci când un astfel de atac apare (este iminent sau în derulare) acea colecție de date și structurile de analiză din „timp de pace" să fie operaționale și în „starea de război". În proiectarea unui echipament similar cu sistemul DEFCON, va fi importantă definirea evenimentelor-indicator ce vor determina automat transmiterea informației spre o structură de analiză a situației.

Epoca armelor atomice a condiționat perfecționarea strategiilor de apărare și de stăvilire a proliferării armelor nucleare. RI diferă de războiul atomic prin numeroase elemente, și de aceea lecțiile învățate din experiență în privința realizării unei strategii funcționale de apărare, nu pot fi folosite în mod direct în problema apărării informaționale, dar cu siguranță pot asigura un punct de plecare pentru considerațiile asupra RI-D.

Unele dintre problemele legate de dezvoltarea apărării împotriva atacurilor RI se referă la diferitele mijloace de ridicare a pragului atacului, folosind un RI ofensiv.

În timp ce ridicarea pragului de apărare este una din componentele specifice oricărei strategii de apărare, (făcând

atacurile mai dificile și mai costisitoare, limitând pagubele posibile), o nouă problemă se pune: ce înseamnă mai multă apărare?

Dat fiind costul mic necesar achiziționării mijloacelor necesare purtării unui RI, actorii nonstatali pot constitui o amenințare strategică. Cum se pot prevedea și împiedica astfel de atacuri?

O altă problemă este cea a naturii acțiunilor care ar putea fi utilizate de către apărare și relația dintre măsurile de contracarare și cele de împiedicare a atacurilor informaționale.

Abilitatea noastră de a apăra sistemele individuale și informația utilizată este fundamentul oricărei strategii și abordări a RI. Pentru a atinge un nivel performant de apărare, trebuie:

1) să revizuim abordarea noastră asupra proiectării și achiziției unui sistem;

2) să înțelegem dimensiunile apărării;

3) să întreținem dezvoltarea unor tehnologii cheie.

Tendința actuală în proiectarea sistemelor este de a asigura un acces lărgit, pentru un număr tot mai mare de informații, la toate nivelele organizaționale. Noua noastră abordare a sistemelor de informație implică un „reach back", ce presupune că indivizii nu „împing" informația, ci mai degrabă „scot" informația cerută, din diversele baze de date. Dirijați de ciclul scurt de viață al tehnologiei informaționale și de bugetele micșorate, devenim din ce în ce mai dependenți de software. Acest lucru face din ce în ce mai greu de asigurat integritatea informației.

Dacă trebuie să construim nivelul apărărilor contra atacurilor RI, trebuie să asigurăm utilizatorii cu nivelul de siguranță cerut, pentru a le da încredere în sistemele lor. De aceea avem nevoie de câteva schimbări în abordarea noastră în privința proiectării sistemului și achiziției. Din mai multe motive, unul dintre ele fiind securitatea, trebuie să ne concentrăm mai mult pe asigurarea

informației de calitate, aceasta însemnând să modificăm continuu relația „date – informație – înțelegere – cunoaștere".

În evaluarea proiectelor de sistem și în stabilirea standardelor pentru sistem, trebuie să creștem setul curent de măsuri de merit („MOMs") pentru informație. Față de atribute ca timpul și acuratețea, trebuie să ne concentrăm în plus pe autenticitate, integritate și valabilitate.

Conexiunea este importantă pentru a atinge nivelurile de funcționalitate dorite, dar o subliniere accentuată a interoperabilității securizate este necesară pentru a realiza obiectivele RI defensiv.

„Operațiile și menținerea activităților" („O&M") asigură oportunități pentru a preveni intruziuni și pentru a întări apărările sistemului. Operatorii de sistem și de menținere a software-ului sunt adesea cei mai puțin experimentați. Dată fiind natura critică a O&M pentru menținerea sistemelor de apărare, practicile O&M trebuiesc revizuite.

Apărarea este o funcție mai mare decât proiectarea și asigurarea calității software-ului. Are multe dimensiuni, unele dintre ele fiind ilustrate în Figura 10. Fiecare dintre aceste dimensiuni trebuie considerată în funcție de fiecare sistem și set de circumstanțe.

În plus față de modul de proiectare a unui sistem, aceste dimensiuni ale apărării includ operații de sistem, metode și proceduri folosite pentru a limita atractivitatea și/sau consecințele unui atac. Figura 10 prezintă câteva dintre dimensiunile apărării care trebuie să fie luate în considerare în construcția unui sistem de apărare informațional.

Fiecare dimensiune oferă un set de alegeri care asigură mai multă sau mai puțină protecție. Mai multă protecție înseamnă un anumit preț (surprinzător, prețul poate fi mic, mai ales dacă îl comparăm cu câștigurile în securitate pe care le putem obține).

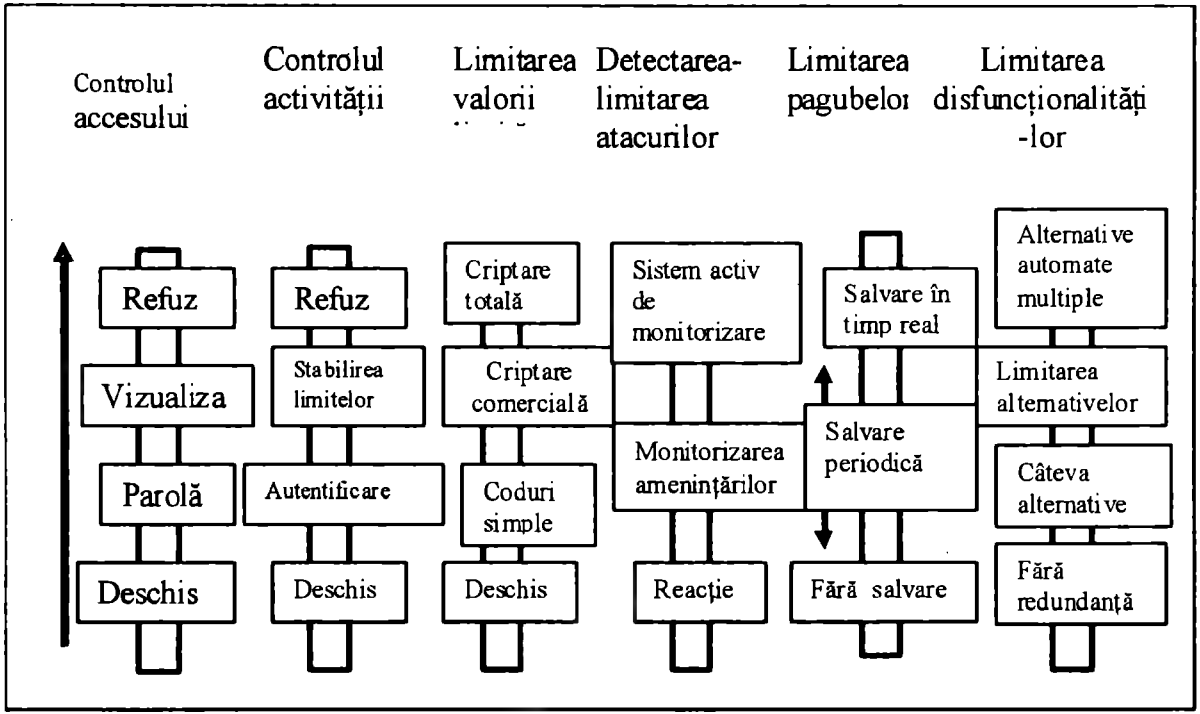


Figura 10. Dimensiunea apărării

Construcția apărărilor presupune existența mijloacelor pentru realizarea acestora. Multe dintre capacitățile de apărare, pe care le avem în mod obișnuit, nu sunt adecvate pentru anumite nivele cunoscute sau tipuri de atac. Acestea sunt domenii unde am putea folosi progresele în tehnologie.

Timpul real de detectare a intruziunii este în mod cert un element-cheie, în orice set de apărări. Capacitatea noastră de a detecta, în timp real, incursiunile în sistemele noastre și identitatea agresorului, este limitată. Nu-ți ia mult timp pentru a susține un atac informațional. Daune pot apărea în orice clipă. Este clar că ar fi de dorit o capacitate automată de a răspunde la o intruziune, care să poată preveni sau limita pagubele.

Dată fiind creșterea confidenței noastre pe COTS trebuie să găsim căi pentru cost - eficiență, pentru a fi siguri că software-ul pe care l-am cumpărat face ceea ce vrem noi și numai ceea ce vrem noi. Orice instituție din Epoca informației cumpără milioane de linii de cod în fiecare an, ale căror origini exacte nu sunt cotate cu nici un grad de încredere. Existența unor instrumente automate pentru a realiza încrederea de calitate și pentru a verifica și valida codul, ar fi de mare ajutor.

A ști cu precizie că datele nu au fost alterate sau compromise și că sursa unei baze de date a fost verificată, ar ajuta mult în efortul nostru de a combate atacurile informaționale.

Piatra de încercare a eforturilor noastre de a combate RI va fi efortul tuturor organizațiilor de a-și proteja propriile sisteme și informația. Unele organizații s-au îngrijit de acest lucru de mai mult timp și au dezvoltat și implementat planuri de a se menține în top, față de creșterea serioasă a setului de amenințări. Alte organizații mai au încă multă muncă de depus în acest domeniu.

Ar putea fi folositoare, chiar și acelor organizații care simt că sunt bine pregătite, revizuirea următoarei liste de acțiuni, pentru a determina ceea ce trebuie făcut, pentru a fi mai bine pregătite pe viitor.

Prima acțiune sugerată implică o revizuire a misiunii organizației în lumina noilor amenințări. Anumite organizații vor

observa că RI-D adaugă o nouă misiune sau crește importanța misiunii existente.

Cine este responsabil cu RI-D în organizație? Poate că organizația are un Ofițer Șef de Informație și ar fi indicat ca acesta să-și asume responsabilitatea. Poate că responsabilitatea RI-D este partajată de mai mulți indivizi. În orice caz, este necesară o alocare clară a responsabilităților.

Nu toate informațiile sau toate sistemele ar trebui considerate egale în ceea ce privește protecția. Este important, date fiind constrângerile de resurse, să identificăm care informație și care sisteme (și funcții ale acestor sisteme) sunt critice și care nu.

Cât de vulnerabile sunt informațiile și sistemele? Care este natura specifică a vulnerabilităților? Răspunsurile sunt necesare pentru a asigura o bază de date pentru a planifica și dezvolta apărările. Trebuie reținut că natura vulnerabilităților evoluează constant. Așadar, analizele vulnerabilităților trebuie să facă parte dintr-un efort continuu.

Acțiuni izolate pentru a îmbunătăți securitatea sunt de ajutor, dar ele nu sunt substitutul pentru dezvoltarea comprehensivă a strategiei RI defensiv pentru organizație. Din moment ce nu este posibil să evităm toate riscurile asociate cu RI, fiecare organizație trebuie să elaboreze un plan de administrare a acestor riscuri.

În cursul dezvoltării și articulării unei strategii organizaționale și a planului de management a riscului în RI defensiv, multe probleme vor fi discutate. Aceste discuții vor crea o mai mare conștientizare a problemei în cadrul organizației și va îmbunătăți abilitatea organizațională de a face față provocărilor asociate cu RI defensiv.

A combate RI este o problemă care trebuie privită pe termen lung. Strategiile de investiție ale unei instituții trebuie revizuite. Unele realocări de resurse pot fi necesare datorită schimbărilor survenite în costurile operaționale și datorită introducerii de noi proceduri și măsuri de protecție.

CONCLUZII

Problema apărării împotriva atacurilor informaționale este reală. Cetățenii noștri și organizațiile care le asigură servicii vitale sunt foarte expuși acestui fenomen. Costul scăzut al acestor atacuri a lărgit câmpul adversarilor potențiali și a complicat eforturile de a strânge informații și de a se apăra. Consecințele unui atac bine planificat și coordonat pot fi serioase. Rămâne de văzut cum va răspunde publicul unei amenințări de atac asupra infrastructurii.

Această situație se accentuează odată cu proliferarea rapidă a tehnologiei informaționale și a competenței în domeniu. Devenim tot mai dependenți de sistemele automate, în fiecare aspect al vieții noastre.

Deoarece tehnologia informațională devine o parte importantă a modului în care organizațiile și indivizii creează, produc și asigură servicii, nevoia de interconexiune și interoperabilitate între acestea crește. Odată cu nevoia crescândă de schimburi de informațiii (și produse), cresc și vulnerabilitățile.

Dată fiind situația actuală, trebuie să ne concentrăm, în principal, asupra a două lucruri. În primul rând trebuie să găsim o modalitate de a ne proteja pe noi înșine de atacurile informaționale și în al doilea rând, trebuie să elaborăm un fundament stabil, care să ne permită să facem progrese sigure, ridicând continuu costul unui atac și limitând paguba așteptată.

OPERAȚIILE INFORMAȚIONALE. CÂTEVA REFLECȚII OPERAȚIONALE SISTEMUL SISTEMELOR

JMJ BOSCH*

Operațiile informaționale pot fi înțelese doar în contextul mai larg al schimbării și continuității. „Ciberspațiul" este asemenea pământului, apei, aerului și spațiului, o dimensiune în care războiul poate fi dus, unde apărarea este o necesitate, în timp ce atacul este o posibilitate. Există o legătură strânsa între „războiul bazat pe informație" și „operațiile informaționale".

Operațiile informaționale n-au impact numai asupra domeniului militar, ele pot de asemenea produce efecte și la nivel național, internațional și chiar global, influențând astfel un stat, o alianță de state sau chiar opinia publică internațională. În cele din urmă la toate nivelele este nevoie de comandă și control pentru a menține ordinea în sistem. Fără a minimaliza importanța tehnologiei, în cele din urmă omul este cel care decide și care acționează.

Dată fiind dependența noastră de tehnologia informațională și de comunicație (ICT) și de opțiunile de a manipula informația, ne confruntăm azi cu noi amenințări; provocarea este aici și acum. Frustrarea este o consecință a complexității schimbării.

Există o listă aproape fără sfârșit de cărți, articole și alte publicații despre informație ca mijloc, țintă sau armă, pe scurt despre „războiul bazat pe informație" și despre „operațiile informaționale".

* Academia Militară Regală, Breda, Olanda.

În al doilea rând, se poate observa complexitatea varietății de schimbări care influențează deja sau vor influența în curând comanda și controlul. Scopul articolului este, în esență, unul de natură militară. În primul rând, tratează perspectiva observatorului militar, care încearcă să înțeleagă prezentul și viitorul, care se confruntă cu schimbări ale vitezei procesării moderne computerizate. Să ne gândim la soluții este singurul lucru care ne rămâne de făcut, pentru a putea înțelege provocarea. Țelul meu este să descriu înțelesul și implicațiile războiului bazat pe informații și operații informaționale pentru a sensibiliza conștiințele [13].

Unii ar putea să susțină că trăim într-o eră a prea multor schimbări. O dată cu dispariția confruntării est-vest, stabilitatea s-a diminuat și a dat naștere mai multor schimbări. Actuala scenă internațională are sute, dacă nu chiar mii de actori care se luptă pentru putere, influență, bani și atenție.

Statele se numără și ele printre acești actori. În această arenă complexă, dezvoltările economice, ecologice, demografice, culturale și tehnologice pot conduce, singure sau în combinație, la conflict. Bogăția este destul de inegal răspândită dacă comparăm estul cu vestul și nordul cu sudul. Există o puternică legătură între creșterea economică și cea demografică.

Schimbări în mai bine survin doar atunci când creșterea economică depășește în mod substanțial creșterea populației. A treia dimensiune este ecologia. Ne confruntăm și aici cu o distribuție inegală de materiale și energie. Apa este o adevărată problemă deoarece nu există nici un fel de substitut pentru această problemă.

Cultura, a patra dimensiune, merită și ea atenție. Acolo unde granița săraci-bogați coincide cu granița culturală, și acolo unde identitatea este în pericol, percepția și convingenle religioase pot

[13] Primele idei în acest sens au fost introduse de autor în lucrarea „operațiile informaționale. Schimbare sau frustrare?", publicată în DSEi Conference Proceedings (1999), vol.2, p. 3-10.

genera forțe cu o dinamică periculoasă. Mijloacele de informare în masă sunt atât spectatori cât și comentatori. Ele sunt uneori strict controlate.

Fiind un pod între „mesaj" și auditoriu, ele influențează sentimentele colective, emoțiile și pot forța decizii, inclusiv în ce privește folosirea forței. Apoi, mai există știința și tehnologia pe temelia cărora orice societate își construiește capacitățile sale de a produce bunuri și servicii - inclusiv de natură militară -, de a organiza și de acționa.

Tehnologia informațională și de comunicații (ICT), combinația de computere și de telecomunicații, afectează toate aspectele de fiecare zi ale vieții, societatea și lumea în care trăim. Biotehnologia este un domeniu promițător atât pentru medicină cât și pentru agricultură sau pentru arme noi.

Tehnologia spațială poate duce la noi opțiuni pentru comunicații, supraveghere și management al mediului înconjurător care poate afecta toate celelalte domenii. Încă din 1998, Centrul de Cercetare Ames, de la NASA, din California, a prezentat un concept pentru un sistem revoluționar de transmisii construit din atomi și molecule. Acest sistem constituie în sine o revoluție: „nanonizarea" mașinilor și sistemelor. Dar cum tehnologia înseamnă putere și bani, ea este o sursă potențială de conflict.

Ea se adaugă la sursele de conflict existente, ca răspândirea inegală a populației, spațiul de locuit, bogăția și apa. O ultimă sursă este chiar istoria în sine, deoarece a lăsat neîncheiate socoteli și a adus - cel puțin unora - ură și supărare. Date fiind aceste observații, definițiile și conceptele tradiționale de securitate sunt tot mai inadecvate.

Cea mai mare provocare a zilelor noastre este să înțelegem lumea complexă în care trăim și tendințele care se prefigurează pentru viitor. Foarte probabil, vor fi tendințe viitoare diferite în funcție de cine suntem și unde trăim. După Van Creveld, trăim în „epoca automatizării", după soții Toffler, suntem parte a celui de-al „treilea val", trăim în „epoca informațională". Atât

schimbarea cât și continuitatea însoțesc omenirea. Constantele sunt lupta pentru putere, influență, bogăție și nevoia continuă de adaptare la o schimbare fără de sfârșit.

Au fost și vor fi dezbateri interminabile despre revoluțiile tehnologice militare. După unii autori, noi o experimentăm acum pe a zecea. Alții folosesc criteriul cronologic pentru a ilustra schimbările revoluționare. Dupuy a descris, folosind drept criteriu viteza și procesul schimbărilor tehnologice, patru perioade [14]. Slipchenko, un general maior rus, a afirmat că războiul din Golf a prezentat o parte din cele șase generații de arme [15]. Van Creveld a descris patru epoci: „epoca uneltelor", „epoca mașinilor", „epoca sistemelor" și cea de-a patra, începând de prin 1945, „epoca automatizării".

După soții Toffler, noi ne aflăm acum în „cel de-al treilea val". O nouă tehnosferă, o nouă sferă a informației, o nouă sferă industrială, instituții noi și noi tipuri de război în care informația are o valoare critică, marchează acest val, ce-și are originile în SUA, în perioada 1955 și 1965.

Există o vastă discuție despre numere, motive, efecte și sens al revoluțiilor. În schimb, nu se discută prea mult despre faptul că cle se produc acolo unde se întâlnește viziunea cu tehnologia în noi concepte, organizări și moduri de operare. În cele din urmă, toate schimbările au fost efectul unei combinații de factori.

Impactul revoluțiilor vine odată cu definiția, este decisiv într-un anumit moment în istorie. Pe termen lung - cu excepția armelor nucleare - revoluțiile tind să fie pietre de hotar în procesul de evoluție. Statele, și prin ele armatele, au obținut mijloace mai sofisticate pentru a le utiliza în conflict.

Cuvântul „revoluție" are un înțeles special. În general, pot fi observate patru tendințe. Prima are de-a face cu depășirea limitărilor fizice și psihice ale ființei umane, a doua cu creșterea vitezei, distanței, preciziei și letalității armelor. A treia se ocupă

[14] Dupuy, volumul 6, p. 2702.
[15] Bowdish, p. 26 și notele de final 4-6.

de protecție. A patra se îngrijește de păstrarea controlului și comenzii, în ciuda armelor noi disponibile, a mediului, a oponentului, a elementului de surpriză.

Soldatul individual tinde să devină, ceea ce corporația RAND numea, „Cavalerul Jedi"; cu un simț supradezvoltat, indestructibil, invizibil și letal. Vom asista la sisteme de senzori, mai mari sau mai mici, care vor folosi unde micro din spectrul radio și fuziuni de date. Ne vom putea aștepta la arme cu energie, precum laserele și armele electromagnetice. Vom vedea arme non-letale noi, mai bune și va exista un spectru de posibilități mai larg pentru a ataca omul, mașina sau softul.

Metodele merită și ele o atenție specială. Unii ar putea găsi noi căi de a utiliza „vechi" metode precum războiul biologic, chimic și ecologic, războiul de guerilla, și, așa cum se va arăta pe parcursul acestui articol, războiul informațional. În cele din urmă, schimbarea în cadrul sectorului militar este întotdeauna legată de tehnologie. Dar războiul și conflictul sunt marcate de numeroase constante.

Ele sunt marcate de voințe, deprinderi și ucideri. Comanda și controlul are întotdeauna de-a face cu incertitudinea și trebuie să găsească căi pentru a evita fricțiunea, „această teribilă fricțiune", așa cum arăta Von Clausewitz. Fricțiunea este mai mult decât efectul fricii, al exhaustivității și incertitudinii despre „ei" și „noi".

Ea are de-a face de asemenea cu norocul, coincidența și ghinionul. Fricțiunea azi este mult mai complicată decât a fost altădată. Clausewitz nu trebuia să se gândească la război aerian, spațial, la războiul de coaliție sau la presă, etc.

În schimb, forțele moderne trebuie să se gândească la toate aceste lucruri. În cele din urmă, mai intervine și elementul surpriză. Esența comenzii nu este să reduci fricțiunea, ci să învingi toate provocările. Ultima constantă este nevoia continuă de adaptare la o schimbare continuă. Constantele sunt într-adevăr legate de om.

În timpul primului război mondial, armatele au ajuns să înțeleagă sensul unei a treia dimensiuni. Al doilea război mondial

a făcut loc celei de-a patra dimensiuni, dimensiunea electronică, alături de care s-a stabilit și dimensiunea psihologică. Tot atunci au început să se lege primele idei despre folosirea spațiului. Noțiuni de genul „ciberspațiu", „sferă informațională" sau „lume digitalizată" fac ca operațiile informaționale să devină o adevărată problemă.

Al doilea război mondial a acționat ca un catalizator pentru multe dezvoltări: război mecanizat, operații combinate, război în apă, sub apă și în aer. Rezultatul a fost introducerea radarului, sisteme noi de comunicare, rachete și computere. Idei timpurii precum cele ale lui Charles Babbage (1792-1871) s-au materializat în concepte precum „motoare de diferențiere" și, în 1834, „motoare analitice".

Hollerith a creat echipamentul de calcul în 1890. În 1939, Atanasoff, un matematician și fizician american, a construit ceea ce unii numesc primul prototip al unui computer electromecanic digital. În 1944 a văzut lumina zilei calculatorul automat cu secvență controlată, Harvard Mark I, care a dus în 1946 la realizarea computerului digital complet electronic, cunoscut sub acronimul de ENIAC.

Pentru mai mult timp, un alt Mark I a fost puțin cunoscut; el a fost dezvoltat la Bletchley, și a fost prevăzut pentru acțiuni împotriva Enigmei, sistemul german de criptare. În 1943, a fost introdus primul Colossus, care utiliza 15000 de tuburi electronice; trei luni mai târziu a apărut Colossus II, cel care i-a dat lui Hollerith ideea unei noi dimensiuni [16].

În ambele armate, atât în cele din Vest cât și în cele din Est, computerul s-a dezvoltat dintr-un lucru rar, uneori chiar secret în ceea ce este el astăzi. Însă dezvoltarea lui nu face obiectul studiului de față. Computerele sau chiar mai bine tehnologia informațională sunt acum „un fapt normal de viață". În același timp, este relevant să observăm că aceste computere sunt mașini.

[16] Lewin, p. 129-133.

Oricine știe că inputuri proaste dau naștere la outputuri pe măsură. Toată lumea ar trebui să știe că nu există program soft fără erori. După Welsh, un program militar standard poate număra 2% fisuri [17]. Așadar nu există o fundamentare reală pentru o încredere absolută în ceea ce un computer „spune". **Ba chiar mai mult. În 1998, o companie germană a dezvoltat un soft care transforma - prin Internet - orice computer personal într-un instrument de spionaj**. Tehnologia informațională și de comunicații influențează armatele moderne, societățile și lumea în general.

Armatele moderne nu pot opera fără așa numita „sferă informațională". Complexitatea crescândă a organizațiilor ca rezultat al diversității sistemelor de arme de înaltă precizie și cu rază lungă de acțiune și creșterea continuă a vitezei, nevoia de intelligence, de coordonare și de sincronizare în combinație cu factorul timp au dat naștere la ceea ce numim noi azi lumea digitală.

Forțele armate sunt administrate, comandate și controlate prin intermediul tehnologiei informaționale și a comunicării. Tehnologia informațională și comunicațiile sunt mai mult decât o combinație de tehnologie computerizată, micro și nano tehnologie, fuziuni de date și inteligență artificială. Aplicarea lor în cadrul sistemului de comandă și combinarea lor stau la baza digitizării câmpului de luptă.

Apoi există națiuni moderne. Prin intermediul tehnologiei informaționale și de comunicații, națiunile moderne organizează guvernul, realizează aprovizionarea cu apă și energie, asigură transportul, reglementează serviciul bancar, finanțele, comerțul ș.a.

Tehnologia informațională și comunicațiile conectează mijloacele de informare în masă cu public diferit. Toate acestea sunt conectate printr-o formă care poartă numele de „infrastructura informațională națională (NII)". În cele din urmă există, o

[17] Welsh, p. 29.

infrastructură informațională internațională, chiar globală (GII), care conectează producători și piețe, bănci și finanțe, guverne și alte organizații, și bineînțeles mijloacele de informare în masă și auditoriul, precum și indivizii.

Internetul cu sutele sale de milioane de utilizatori este doar un element din această infrastructură. Națiunile sunt doar una dintre categorii printre multele instituții și alți actori care aparțin acestor sfere supranaționale. Tehnologia modernă face posibilă lărgirea rapidă a mediului.

O mică invazie a reporterilor de televiziune, radio, a oficialilor guvernamentali și non-guvernamentali împreună cu mijloacele lor de comunicare conectează pur și simplu acel mediu la o infrastructură informațională la distanță. Această combinație de infrastructuri informaționale militare, naționale, internaționale, globale și mediul creează acel ceva ce poate fi numit „ciberspațiu".

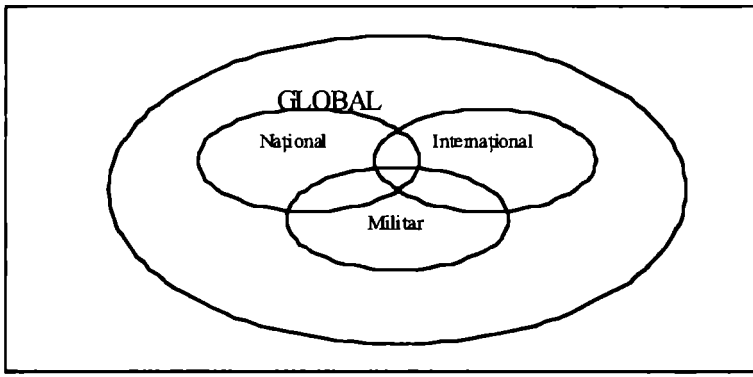


Figura 1: Informația despre mediul înconjurător

În cadrul acestui spațiu, se poate duce război la fel ca și pe pământ, pe mare, în aer sau în spațiu, având drept instrument de acțiune directă, comanda și controlul. Suntem martorii unei noi dimensiuni de război: dimensiunea electronică și psihologică au început să pălească. În cadrul acestui ciberspațiu, operațiile informaționale au de jucat un rol crucial.

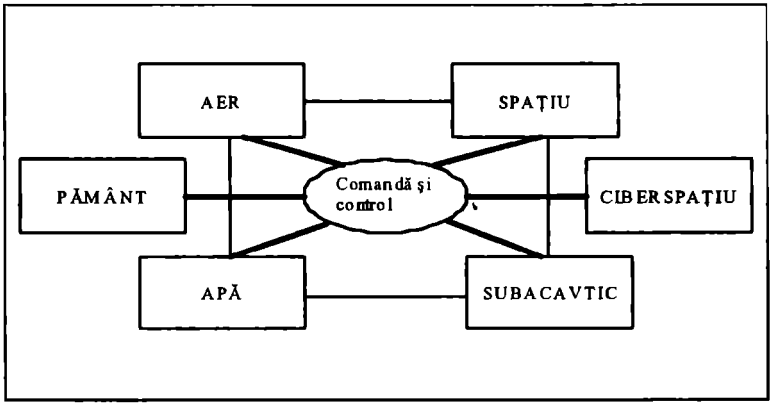


Figura 2: Dimensiunile războiului

Înainte de a începe analiza conflictului în această dimensiune câteva remarci asupra războiului bazat pe informație se impun.

În conformitate cu „Joint Vision 2010", forțele armate care folosesc „sistemul sistemelor" vor câștiga cunoașterea spațiului de luptă și vor putea răspunde la timp. În conformitate cu TRADOC Pamphlet 52505, toate activitățile vor produce în cele din urmă o „Forță totală", capabilă să conducă un război terestru.

Această forță va avea cinci caracteristici: flexibilitate doctrinară, mobilitate strategică, adaptare și modularitate, conectivitate integrată, multinațională și conectivitate interagențială și versatilitate.

Sistemul de comandă se bazează pe noi căi de a folosi tehnologia informațională și de comunicații. Comandanții vor avea o imagine comună, relevantă a bătăliei. Concentrarea se realizează pe spectrul supremației. Combinând aceste dezvoltări cu concepte de operații în adâncime și atac simultan se creează un mod dinamic de a extinde bătălia în spațiu, timp; de reducere, dacă nu chiar eliminare, a timpului și nevoii de modulare a câmpului de luptă. Acesta este mesajul [18].

[18] Pentru mai multe detalii a se vedea Morris J., Boyd și Michael Woodgerd.

Dar dezvoltările merg chiar și mai departe. În anul 2025 ar trebui să existe ceva de genul „Internet viu". După Perricelli, ar trebui ca fiecare individ de pe câmpul de luptă să poată interacționa în orice moment, în timp aproape real. Această așa numită „Sferă informațională " asigură transport informațional și servicii informaționale luptătorilor, independent de localizare, grad de mobilitate sau dinamică platformelor [19].

Ecranele computerelor și băncile de date nu dau imaginea în totalitate. Unele aspecte precum motivarea, estimările, sentimentele, personalitatea și cultura sunt greu de depozitat sau de vizualizat. Dacă vorbim despre oameni implicați într-un război real, este recomandabil să citim „Military Misfortunes" de Eliot A. Cohen și Richard Gooch. Mulți militari uită să traducă experiențele în acțiune.

Apoi, există fluxul și folosirea informației. Doar datele și informațiile nu pot susține deciziile. Iar și iar, omul va trebui să selecteze, să analizeze, să interpreteze și să evalueze pentru a putea decide și acționa. Se poate astfel ajunge și la forme de „patologie informațională".

Prăpastia între ceea ce putem ști și ceea ce putem cunoaște se adâncește. Abilitatea de a produce informație a crescut; abilitatea de a procesa informație nu s-a îmbunătățit. Fluxul suplimentar de informație induce sentimentul de „fără putere".

Într-un experiment, 1313 manageri din mai multe țări și-au exprimat părerea asupra informației.: 49% erau adesea neputincioși să digere informația valabilă; 65% se așteptau ca viitorul să aducă mai puțin stres [20].

O mașină este logică, „omul" este logic doar uneori. Omul diferă în multe privințe de o mașină. În termeni logici, el (sau ea) este inferior. Nu este surprinzător că în cele din urmă computerele

[19] Perricelli, Robert F. P. 34-39.
[20] „Dying for information", Executive Summary

reușesc să-i bată la șah pe marii jucători. Unele acțiuni și contra-acțiuni în război pot fi definite în termeni logici: o rachetă ce vine, dirijată prin radar în combinație cu o armă defensivă.

Dar multe acțiuni într-un război sunt în afara acestui tărâm. În acest context, omul este cel mai prețios dar și cel mai limitat factor. Cel mai prețios pentru că creativitatea și sentimentele contează atunci când este vorba de un conflict. Limitat, pentru că omul depinde de caracterul său, de informații, de mediul înconjurător și de experiență.

Comandantul are de-a face cu un set complex organizațional, fizic, interpersonal și psihologic, care este controlat de cerințe și reguli ale misiunii, de climă și oboseală, de relațiile de comandă și de afinități cu tovarășii de luptă, de ambiție și de frică.

SISTEMUL SISTEMELOR. În primul rând, el dă o viziune comună a câmpului de luptă. A vedea același lucru pe ecranul unui computer, nu înseamnă a împărtăși aceeași interpretare. Imaginea mediului inconjurător este colorată de ceea ce știm, de ceea ce nu știm, de ceea ce credem că știm și de ceea ce credem că nu știm, dar, de asemenea, și de caracterul și cunoștințele celor care împart ecranul și de circumstanțele cu care ei se confruntă.

În al doilea rând, viteza. Cum putem combina acțiuni la diferite nivele, atât pe orizontală cât și pe verticală, astfel încât viteza să fie sincronizată? O diferență în viteză poate conduce la pierderea momentului, la luarea de decizii pripite sau chiar în sens larg, la punerea în pericol a comenzii și controlului.

În al treilea rând, comanda și controlul. Situația de avertizare a tuturor poate fi în același timp și o binecuvântare și un blestem. Pe de-o parte, pot să existe neînțelegeri asupra persoanei care trebuie să decidă, asupra a ceea ce trebuie să decidă, asupra celui care stabilește prioritățile și dă ordinele.

Pe de altă parte, există riscul micro-managementului. Sincronizarea este cheia acțiunilor integrate. Nu numai procesul

este cel care contează - organizarea acțiunii în termeni de spațiu și timp - dar și efectul, rezultatul pe care-l dorim. Nu există acțiune integrată fără coordonare și sincronizare; realitățile spațiului de luptă pot uneori să necesite inițiativă și răspuns imediat.

În al patrulea rând, celelalte efecte. Într-o unitate pe deplin digitizată nu există hărți reale, cu greu se găsesc instrucțiuni sau ordine scrise. Acest lucru înseamnă că viteza într-o asemenea unitate depinde de cel mai puțin digitizat element.

Dacă sistemul eșuează, comanda și controlul pot ajunge într-un punct mort deoarece totul se bazează pe informație computerizată fără nici o alternativă. Harta militară cu o gaură în interiorul ei este totuși o hartă, pe când dintr-un computer în care s-a tras un glonț nu mai rămâne nimic. Există trei tipuri de asimetrie tehnologică: Prima este atunci când partenerii dintr-o coaliție se bazează diferit pe tehnologie. A doua se manifestă atunci când partenerii se bazează în egală măsură pe complexul tehnologic dar utilizează forme diferite. A treia variantă apare atunci când partenerii, care se bazează în egală măsură pe tehnologie similară, o folosesc în diferite scopuri.

În al cincilea rând, pot oamenii să se încreadă în sisteme și în informațiile pe care acestea le produc? Așa cum s-a arătat și mai înainte, omul nu este computer și este supus distorsionărilor datorită emoțiilor și motivațiilor. El poate de asemenea să fie victima manipulării. Cum se poate preveni degradarea semnificativă sau, chiar mai rău, manipularea? Cum se poate „ataca" un adversar? Cum se poate opera în cadrul mediilor informaționale înrudite? Răspunsul la aceste întrebări poate fi găsit în cadrul complexului modern de realități a comenzii și controlului.

În literatura de specialitate, așa numita „OODA-loop" (Observare, Orientare, Decizie și Acțiune) este adesea folosită pentru a ilustra procesul și ciclul de comandă și control (C2).

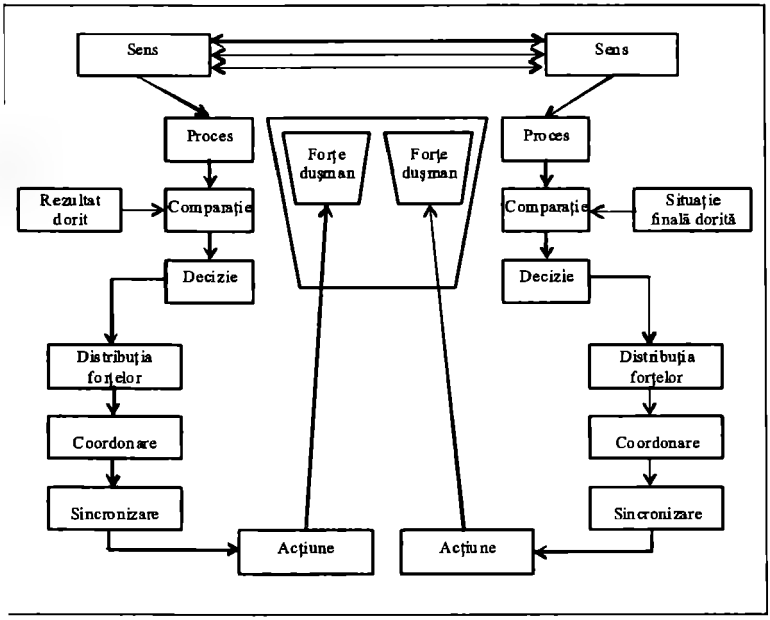


Figura 3: *Cele două cicluri de comandă-control opuse*

În realitate, o organizație militară în acțiune este o mașinărie complexă unde sute, chiar mii de celule la diferite nivele de organizare - fiecare având propria viteza - trebuie să fie coordonate și sincronizate. Viteza fiecărei celule este influențată de calitatea proprie, de aranjamentele organizaționale, de tehnologia disponibilă, de complexitatea problemelor care trebuie rezolvate și de circumstanțe.

Coordonarea cu un singur element se poate realiza într-un imp foarte scurt. Dar coordonarea și sincronizarea mai multor celule presupune o altă dimensiune. În cele din urmă, și poate cea nai importantă considerație: OODA-loop a fost introdus pentru a ezolva o problemă; C2 are alt scop. Figura 3 prezintă o ilustrare ealistă a procesului și ciclului de C2 în cea mai simpla situație: ea a doi comandanți care se opun [21].

[21] Lawson a pus bazele în 1977. Hughes a introdus combinația celor două cicluri: cea aliată și cea dușmană (Hughes, p, 187). Autorul a introdus istribuția forței, coordonarea și sincronizarea ca elemente esențiale.

Dar chiar și această ilustrare este o simplificare. Nu acordă prea mare importanță faptului că există mai multe cicluri la diferite nivele. De asemenea neglijează faptul că mulți se preocupă în același timp cu protejarea și susținea forțelor, cu treburile administrative, precum și cu planurile acțiunilor viitoare. Ambele cicluri au ca scop să susțină acțiunea și să influențeze sau să neutralizeze oponentul. Finalitatea comenzii este menținerea controlului. Acest lucru reprezintă mai mult decât a susținut Van Crefeld, „reducerea incertitudinii"[22]. Criterii pentru un sistem perfect de C2:

- Păstrarea ordinii și coeziunii ropriilor forțe;
- Controlul spațiului de luptă și evitarea ciocnirilor fatale;
- Optimizarea alocațiilor, strategiilor sau compoziției forțelor[23].

COMPLEXUL DE COMANDĂ ȘI CONTROL (C2C) O generalizare acceptabilă pentru ceea ce înseamnă „informație" poate fi exprimată astfel: „cea care reduce incertitudinea"[24], cu alte cuvinte, date atent selecționate, organizate, relevante și - ori de câte ori este posibil - la timp.

Sistemul informațional funcționează precum venele și nervii unui complex mai larg de comandă și control. Procesul de comandă și control traduce date și informații în ordine. Într-un sens mai restrâns, orice sistem informațional modern are șapte componente de bază; „senzori, procesori, receptori, date și informații, baze de date, transmițători și reguli". În esență, comanda și controlul sunt sprijinite de către un sistem C2. Complexul de comandă și control (C2C) cuprinde totul: factori de decizie, hardware și software, infrastructură.

---

[22] Van Crefeld, p. 235-249.

[23] Hughes, p. 191 referindu-se la Welch așa cum este citat în Hwang la p. 4-6.

[24] Dixon, p. 28

Tabelul 1 arată într-o manieră ce separă, elementele celor două părți opuse:

Apărare proprie	Atac
Senzori, procesori, receptori, baze de date, transmițători	Senzori, procesori, receptori, baze de date, transmițători.
Infrastructură, putere, transport	Infrastructură, putere, transport
Date, informații, software, reguli	Date, informații, software, reguli
Comandanți, consilieri şi alți susținători ai sistemului	Comandanți, consilieri şi alți susținători ai sistemului
Trăgători, alți actori şi utilizatori	Trăgători, alți actori şi utilizatori

Informația a fost din totdeauna importantă; chiar în Biblie putem citi că spionii au fost folosiți în recunoașterea terenului și observarea inamicului. C2 a fost din totdeauna o țintă. Calul Troian este un bun exemplu de inducere în eroare de timpuriu. O dată cu dezvoltarea conceptului de C2, noi opțiuni de atac au fost găsite. Această înțelegere a condus la apariția conceptului de război de comandă și control (C2W).

În cadrul NATO, războiul de comandă și control este definit ca *„folosirea integrată a distrugerii fizice, a războiului electronic, inducerii în eroare, operațiilor psihologice și de securitate, sprijinite de către intelligence pentru a interzice adversarului accesul la propriile informații, influențarea, degradarea, confuzia sau chiar distrugerea capacităților de C2 ale adversarului și pentru protejarea partenerilor împotriva unor astfel de acțiuni"*[25].

Obiectivele măsurilor de război de comandă și control constau în deschiderea, menținerea sau chiar lărgirea diferențelor de eficiență a C2-ului în favoarea forțelor aliate. Războiul de comandă și control ofensiv este eficient, mai ales în domeniul economic pentru reducerea luptei adversarului. Este aplicabil la toate nivelele de comandă. Obiectivele primare ale războiului de comandă și control împotriva potențialului de luptă al unui dușman constau în:

- Încetinirea tempoului operațiilor sale;
- Întreruperea operațiilor sale;
- Degradarea ciclului C2 de comandă al dușmanului;
- Distrugerea abilității sale de a genera putere de luptă;
- Scăderea dorinței sale de luptă.

Prezervarea sistemelor prietene de C2 - războiul de comandă și control defensiv - este o considerație fundamentală, deoarece eșecul este foarte probabil să conducă la pierderea libertății de acțiune și inițiativei, la o redirecționare a efortului sau chiar la eșecul operației. Obiectivele primare ale războiului de comandă și control defensiv constau în:

[25] ATP 35 (B), capitolul 2. A se vedea de asemenea MC-348.

• Reducerea vulnerabilităților elementelor de C2 pentru atac;

• Reducerea efectelor operațiilor de securitate inamice împotriva sistemelor C2 prietene;

• Neutralizarea efectelor acțiunilor de război electronic împotriva sistemelor prietene de C2;

• Împiedicarea inamicului de a exploata sistemele C2 prietene;

• Ineficientizarea acțiunilor psihologice inamice.

Deși războiul de comandă și control indică „prezervarea sistemelor de C2 prietene", este clar că adevărata sa preocupare este „comanda și controlul" în întregul său.

Distrugerea fizică nu mai are nevoie de precizări suplimentare.

Războiul electronic include efortul de a câștiga intelligence prin observarea și evaluarea folosirii de către dușman a spectrului electromagnetic [26]. Inducerea în eroare constă în manipularea dușmanului, distorsiunea, falsificarea evidenței pentru a-i sugera să reacționeze într-o manieră contrară intereselor sale.

Scopul de bază al inducerii în eroare ofensive este de a obține surpriza și de a menține inițiativa. Scopul de bază al măsurilor defensive este să îmbunătățească securitatea și să stabilească condițiile pentru operațiile viitoare [27]. Inducerea în eroare trebuie direcționată spre o țintă umană, care este de regulă comandantul inamic și staff-ul său și se bazează pe reacțiile lor posibile.

Operațiile psihologice au trei scopuri: să slăbească dorința adversarului, să câștige sprijinul celor nehotărâți, să întărească loialitatea celor care sunt deja adepți declarați. Operațiile psihologice trebuie coordonate cu informarea publică, cu activitățile civile.

Nu există o definiție universal acceptată pentru conceptul de „operații informaționale". Americanii în documentul FM 100-6, din iunie 1996, defineau operațiile informaționale astfel:

Operații militare permanente în cadrul MIE (Military

[26] P.2-35.
[27] P.2-36.

Information Environment) care dau posibilitatea, întăresc și protejează abilitatea forței aliate de a culege, procesa și acționa asupra informației pentru a obține avantaj față de toate categoriile de operații militare; Operațiile militare presupun interacțiunea cu GIE (Global Information Environment) și exploatarea capacităților adversarului de informare și decizie sau chiar sabotarea procesului acestuia, de luare a deciziilor prin împiedicarea accesului său la informații.

Departamentul american al apărării a venit și el cu o definiție a operațiilor informaționale: *acțiuni întreprinse pentru a afecta informația adversarului și sistemele informaționale în timp ce sunt apărate informațiile și sistemele proprii.*

Cea mai recentă definiție (publică) americană se găsește în doctrina USAF : *Operațiile informaționale sunt potrivite pentru orice tip de acțiune militară, atât pe timp de pace cât și pe perioada unui conflict. Forțele aeriene sunt convinse că pentru înțelegerea deplină și achiziția superiorității informaționale, înțelegerea noastră asupra operațiilor informaționale trebuie să includă doi piloni conceptuali distincți dar care interrelaționează unul cu celălalt: informația în război - aspectele de „câștig" și „exploatare" sau alte procese ce se bazează pe informație - și războiul informațional - aspectele care se referă la „atac" și „apărare".*

Războiul informațional (RI) este alcătuit din operații informaționale conduse pentru apărarea propriilor informații și sisteme informaționale sau pentru atacarea și afectarea informațiilor și sistemelor informaționale ale adversarului. Aspectul de apărare este operativ tot timpul.

În schimb, aspectul ofensiv se manifestă în primul rând pe timp de criză sau conflict. Războiul informațional presupune activități diverse precum operațiile psihologice, inducerea în eroare, războiul electronic, atacul atât fizic cât și informațional (ciber-atacul) și o întreagă gamă de activități și programe defensive. Este important de subliniat faptul că războiul informațional este o construcție care operează atât pe timp de

pace cât și de război, pentru a permite executarea efectivă a responsabilităților Forței Aeriene [28].

Reflectând asupra acestor definiții trebuie să subliniem faptul că ele într-adevăr diferă. Cu toate acestea, ele au un element comun: informația și sistemele informaționale. Toate definițiile se axează pe realizarea superiorității informaționale. Prin superioritate informațională se înțelege *„capacitatea de a culege, procesa și disemina un flux continuu de informații în timp ce este exploatată sau chiar interzisă abilitatea adversarului de a face același lucru."*[29]

Informația seamănă mai degrabă cu un bun. Ea capată înțeles dacă este folosită în acțiune. Informația poate conduce la înțelegere și la introspecție. Aceasta din urmă, împreună cu înțelesul, timpul și spațiul, ar putea să creeze și să păstreze libertatea de acțiune și să realizeze comanda și controlul efectiv. „Ultra" (sistemul german de decodificare a semnalelor) și „Magic" (sistemul japonez de decodificare) din al doilea război mondial, n-au făcut propriu-zis nimic, nu au ucis pe nimeni, n-au scufundat nici un vas și n-au doborât nici un avion.

Pentru aceste lucruri au fost necesare oameni și mașini. Dacă cineva acceptă că există ceva ce poate fi numit „ciberspațiu", atunci conceptul de „ciber-superioritate" nu poate fi decât acceptat, cu toate că are o natură abstractă și are un înțeles doar în combinație cu alte elemente precum semnificație, timp și loc. Care este adevăratul înțeles al superiorității informaționale?

În cele din urmă înțelegerea, cel de-al șaptelea simț este ce care contează. Jucătorii de șah au toate informațiile la îndemână și cu toate acestea pot să nu înțeleagă ce presupune o anumită mișcare. Războiul este mult mai complicat decât șahul. În lume conflictului există mai multe dimensiuni, una dintre părți deține mijloacele de a influența una sau mai multe dimensiuni și exist

[28] AFDD 2-5.

[29] Bunker, p. 13, nota de subsol 31.

reguli, unele ce decurg din limitările tehnologice, altele ce țin de legea războaielor, de considerații etice.

Dar aceste reguli nu fac legea. Ele pot sau nu să limiteze o serie aproape fără de sfârșit de opțiuni. Că să-l citam pe Holcomb, operațiile militare „nu sunt mecanice, iar comanda și controlul reprezintă mai mult decât pur și simplu urmărirea de proceduri stabilite sau culegerea a cât mai multor informații".

Ipotezele digitizării armatei (dacă, în cadrul unei forțe digitizate, diferite tehnologii și doctrine sunt integrate, așa cum trebuie, în cadrul forțelor, atunci creșteri în letalitate, șanse de supraviețuire și ritm vor fi câștigate) se pot baza pe falsa presupunere că operațiile militare sunt mecanice. Ele sunt – așa cum indica și Clausewitz – descrise ca contracarând fricțiunea.

De aceea, întregul concept de digitizare poate fi o conceptualizare simplistă. Însă, aici trebuie făcută o diferențiere între diverse forțe. Până la un anumit nivel, operațiile aeriene și maritime pot fi descrise ca mecaniciste. Platformele, armele și sistemele lor pot fi descrise în termeni de viteză, înălțime, acuratețe. Dar numărul „actorilor", interacțiunea cu elementele adverse, care pot folosi inducerea în eroare sau să acționeze într-o manieră imprevizibilă și interacțiunea complexă dintre om, mașină, vreme, teren, pune anumite limite predicției.

Simulările pe computer nu pot să stăpânească gândirea și creativitatea comandanților; deciziile lor sunt greu de replicat. Atunci există riscul să credem că având destulă informație și comunicații bune, putem, așa cum spune Holcomb: „să precizăm totul despre dușmanul nostru, iar ceea ce mai rămâne este doar o funcționare eficientă a sistemului pe care noi îl controlăm".

În aceste condiții este doar o chestiune de timp până în momentul în care dușmanul se va recunoaște înfrânt. După părerea sa, „scopul C2 nu este dominarea informațională, ci crearea, ulcătuirea și distribuirea puterii de luptă, în timp ce este acceptată ideea că incertitudine există întotdeauna. Digitizarea nu trebuie să fie niciodată un scop în sine.

Mai există încă o considerație. Ce s-ar fi întâmplat dacă în timpul primului război mondial, celui de-al doilea război mondial, forțele ar fi cunoscut toate detaliile? Cunoașterea poate fi un înlesnitor, dar cu siguranță poate fi și o povară.

Și o altă chestiune. Să presupunem că știm dar suntem împiedicați să ne folosim cunoașterea din cauza inducerii în eroare, a secretului sau a altor implicații. Limitate la domeniul militar, operațiile informaționale includ toate elementele de C2W. Dar acestora li se mai adaugă noi opțiuni: folosirea de arme HERF și de bombe EMP. Apoi mai sunt virușii și alte mijloace de manipulare a informației. Pregătirile și operațiile militare nu se materializează într-un vacuum.

Această legătură cu mediul înconjurător justifică denumirea de „război în rețea" („netware"). Acest război dorește să *„întrerupă, să modifice ceea ce populația țintă știe sau crede că știe despre ea însăși și despre lumea înconjurătoare"*.

În literatura de specialitate, acest concept de influențare a factorilor de decizie, fie direct, fie indirect, prin intermediul publicului larg, mai poartă și numele de „război de percepție" sau „război neocortical". De fapt, el este strâns legat de arta propagandei. Vechi concepte și noi instrumente se întâlnesc, pentru a manipula adevărul. Chiar și în ziua de azi, nu există nicio garanție că o anumită imagine reflectă realitatea, că anumite cuvinte au fost rostite întradevăr. Adevăratele ținte rămân în continuare factorii de decizie.

Strategii ruși susțin: *„Războiul informațional este o cale de rezolvare a unui conflict dintre două părți. Scopul este ca una dintre părți să câștige și să păstreze avantajul informațional asupra celeilalte. Acest lucru poate fi realizat, prin exercitarea unei influențe informaționale/psihologice și tehnice, specifice, prin sistemele naționale de luare a deciziei, prin intermediul populației, prin structurile informaționale, ca și prin înfrângerea sistemului de control al dușmanului, a structurilor sale informaționale cu ajutorul unor mijloace suplimentare, precum armele, materialele nucleare."*[30]

[30] Grau și Thomas, p. 508.

Operațiile informaționale mai pot avea și altă dimensiune. Așa cum indica și Harcknett acest gen de operații pot fi folosite pentru „întreruperea sau distrugerea legăturilor cu societatea, prin ținte precum transportul, comunicarea, energia și instituțiile financiare"[31].

Corporația RAND scrie despre *„folosirea ciberspațiului pentru afectarea operațiilor militare strategice și pentru aducerea de prejudicii infrastructurilor informaționale naționale"*[32]. Un astfel de atac asupra societății poate avea consecințe foarte grave. Nu este nevoie de prea multă imaginație pentru a înțelege ce înseamnă, de pildă, oprirea aprovizionării cu energie pentru societatea modernă.

Tabelul 2 oferă câteva exemple de elemente vitale pentru asigurarea comenzii și controlului în cadrul Statelor Unite.

- Culpepper Switch – se ocupă de toate transferurile electronice ale fondurilor federale;
- Electronic Switching System (ESS) – administrează tehnologia Internet;
- Time Distribution System – de care depind toate rețelele de calculatoare;
- Global Positioning System - GPS;
- World Wide Military Command and Control System (WWMCCS);
- Principalele legături de satelit (Suitland, Bolling);
- Federal Reserve Computing System;
- Submarine Communication Center;

Rețeaua de televiziune

În acest context, nu este deloc surprinzător faptul că multe țări studiază aceste riscuri potențiale. Întrebarea care se pune acum:

[31] Harcknett, p. 95-96.
[32] Molander, Riddle și Wilson, p. 84 și nota de subsol 1.

există sau nu o contradicție în a avea atât conceptul de război de comandă-control cât și conceptul de operații informaționale?

Pâna la un anumit punct, răspunsul poate fi da; ambele concepte se concentrează pe comandă-control, ca pe ceva ce poate fi atacat sau apărat. Există însă și câteva argumente care au contribuit la noul concept, acela de operații informaționale. Primul este legat de dependența crescândă a organizațiilor militare de tehnologia informațională și de comunicații.

O mare parte din calitatea finală a complexului de comandă-control depinde de calitatea datelor, de receptarea lor în timp oportun, de software și de legislații. Există acum noi mijlolace de manipulare și de distrugere a acestor facilități. Conceptul prezent de C2W nu ia în calcul ceva de genul unui atac de software. Al doilea argument ar fi cel legat de faptul că operațiile informaționale nu se limitează doar la vremuri de criză sau conflict. Acțiuni asupra sistemelor de comandă-control și asupra informației au loc acum.

Mai multe țări au raportat activități ale hackerilor, crackerilor și activități controlate, probabil, de grupuri sau state, cu intenția de a pătrunde în sisteme, de a descoperi parole și de a accesa informația. Interconexiunea cu diferite medii informaționale creează vulnerabilități, care pot fi exploatate în orice moment. Ținta poate fi societatea sau chiar comunitatea internațională, așa cum se arăta și în figura 4.

Al treilea argument se leagă de constatarea că nu mai există granițe clare între noțiunile de prieten și dușman. Realitatea politică complexă aduce în prim plan oponenți, susținători ascunși, aliați în diferite forme, neutri. Această realitate înlesnește folosirea cu succes a războiului psihologic și a propagandei chiar și în afara unui conflict armat. Acest lucru forțează națiunile să-și reconsidere poziția lor față de mass-media sau de folosirea sau nefolosirea informațiilor. Un alt argument este legat de conceptele de coordonare și sincronizare. Conceptul de C2W necesită „folosirea integrată a cinci acțiuni militare principale: distrugerea fizică, războiul electronic, inducerea în eroare, operațiile psihologice și

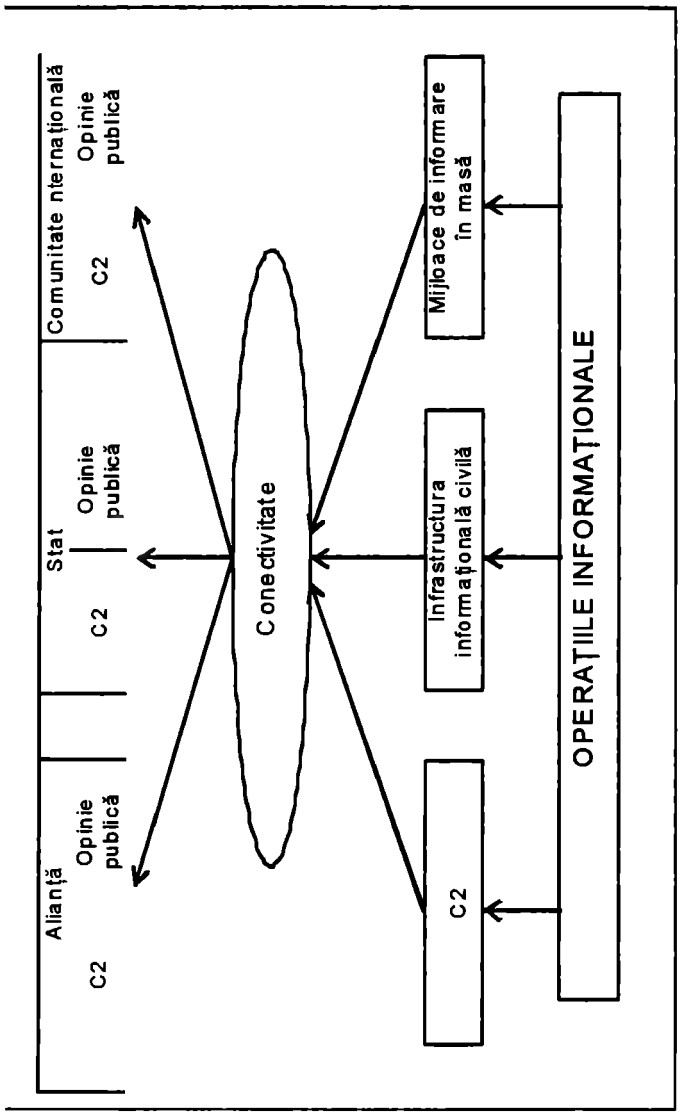


Figura 4: Scopul operațiilor informaționale

OPSEC. De asemenea, acest concept mai subliniază și importanța coordonării operațiilor psihologice cu informația publică, treburile civile și activitățile CIMIC. În lumea în care trăim, orchestrarea cere o concentrare clară, un nou concept și noi linii directoare. Bosnia Herțegovina și conflictul din Cecenia sunt lecții din care trebuie să învățăm.

Războiul din fosta Iugoslavie este un bun exemplu pentru a sublinia complexitatea operațiilor de pace. Scopul lor este să producă condițiile care să conducă la pace și nu să distrugă dușmanul. Dușmanul reprezintă chiar conflictul în sine.

Transparența este necesară că o măsură de încredere și de securitate. Prima companie de operații informaționale pentru Statele Unite, în Bosnia Herțegovina, companie care a urmărit îndeaproape noua doctrină de operații informaționale a armatei SUA, a început în octombrie 1996 în cadrul diviziei multinaționale din nord (Task Force Eagle). LIWA (Land Information Warfare Activity) de la Fortul Belvoir, VA, a constituit punctul central al celulei de operații informaționale din divizie.

Un grup de lucru pe operații informaționale a inclus reprezentanți ai G2, G3, G5, Afacerile Publice, consilieri politici, operații psihologice, etc. Acest grup a planificat întregul efort pentru desfășurarea de operații informaționale, a stabilit prioritățile și a determinat disponibilitatea resurselor operațiilor informaționale.

Mediul de desfășurare al activității aduce în prim plan noi probleme în ce privește informația și intelligence-ul. Există multe părți implicate și toate sunt importante. Toate părțile pot folosi radioul, televiziunea și alte mijloace de informare în masă, prin care să răspândească informația, care poate fi adevărată, parțial falsă sau falsă.

Apoi există mediul internațional care se concentrează pe situație. Toate sursele trebuie monitorizate pentru a fi avertizați din timp asupra situației. Apoi există fluxul normal de informație și intelligence. Toate acestea trebuie culese, analizate și folosite, fie în rapoarte sau baze de date, fie pentru acțiuni directe.

Mai sunt, de asemenea, implicate și operațiile de securitate (OPSEC). Din nou, absența unui dușman clar a creat probleme de securitate. Orice salariat civil poate fi activ pentru una dintre părți. Chiar și cooperarea internațională a creat unele probleme din cauza diferitelor percepții, proceduri sau efecte ale combinării de diferite sisteme automate și de comunicații. Experiențele Forței de Intervenție Vulturul (Task Force Eagle) aduc importante precizări conceptuale asupra organizării, folosirii și limitelor operațiilor informaționale [33].

Războiul din Cecenia (1994-1996) poate furniza indici importanți asupra complexității „conflictului bazat pe informație". Atât Rusia cât și cecenii au folosit operațiile psihologice (PsyOps), inducerea în eroare, managementul percepției și războiul electronic. Exemplele indică că poate să existe o dimensiune specifică care merită un studiu aparte: asimetria.

Lumea super-tehnologizării se confruntă cu o dilemă. Nu se poate vorbi de progres în absența digitizării; dar fiecare pas spre digitizare creează noi vulnerabilități. Războiul este cu siguranță mai mult decât o ciocnire de tehnologii. Este un fapt demonstrat că superioritatea tehnologică nu este o garanție pentru victorie.

Strategii americani spun: **„supremația tehnologică n-a putut împiedica înfrângerea Olandei în Indonezia, a Franței în Indo-China și Algeria, a Americii în Vietnam, a Uniunii Sovietice în Afganistan, a Rusiei în Cecenia. Toate aceste episoade confirmă faptul că superioritatea tehnologică nu este o garanție automată a victoriei pe câmpul de luptă, și cu atât mai puțin la masa negocierilor"** [34].

Nu este nevoie de milioane de dolari și de sute de soldați pentru a ataca „Sistemul sistemelor". Este de asemenea clar că este într-adevăr greu să dezvolți arme noi care să-l surprindă pe dușman. Tehnologia este importantă, dar nu decisivă. Adevăratul război sau conflict este mai înainte de orice o ciocnire a voințelor, iar în acest sens aspectele culturale pot domina.

[33] Task Force Eagle.

[34] Van Riper, Paul K. și Robert H. Scales Junior, p. 4-5.

Un lucru este cert: națiunile și coalițiile trebuie să studieze adevăratele implicații ale operațiilor informaționale. Teoretic, ele pot aduce forme de conflict în care rolul războiului convențional să fie marginal, dacă nu chiar zero. Există două cauze pentru acest lucru: caracteristicile operațiilor informaționale și posibilele efecte.

Prima observație este costul scăzut al unui atac asupra sistemelor informaționale și comunicațiilor în rețea. Acesta este de-a dreptul trivial în comparație cu mijloacele militare convenționale. O combinație de computere și câteva minți strălucite și pline de imaginație este suficientă.

De fapt, noi suntem azi, proprii noștri dușmani, atunci când întărim interoperabilitatea, când reducem măsurile de protecție pentru a mări viteza, când apelăm la standardizare și căutăm să facem economie. Toate aceste mecanisme, într-un anume fel, favorizează un intrus.

Factorul timp se reduce mai mult sau mai puțin la zero. Dacă un atac convențional cerea timp pentru a fi organizat, iar forțele să fie pregătite și dispuse, un atac prin computer poate să înceapă în câteva secunde după decizia lui. Același lucru se întâmplă și cu distanța.

La toate acestea se mai adaugă și faptul că operațiile informaționale sunt realizate mai mult sau mai puțin fără vărsare de sânge. Colapsul sistemului financiar, blocarea aprovizionării cu energie sau căderea computerelor în sistemul militar de aprovizionări poate avea efecte devastatoare, dar toate acestea nu arată - cel puțin la prima vedere - răni și moarte.

O combinație a unui astfel de atac cu manipularea informațională poate avea efecte serioase. Manipularea informațională se poate concentra pe crearea de percepții diferite dintre guvern și populație; poate genera neîncredere la nivel guvernamental și poate pune în pericol existența coalițiilor. În cele din urmă, un guvern poate fi paralizat.

O ultimă chestiune este faptul că operațiile informaționale pun sub semnul întrebării conceptul separării dintre instituțiile militare și civile și ideile noastre de distribuție a puterii.

CONCLUZII. Operațiile informaționale pot fi înțelese doar în cadrul întregului complex de schimbări. Ele nu influențează doar sectorul militar, dar și întreaga societate și comunitatea internațională. Unul dintre efectele tehnologiei informaționale și comunicaționale este crearea a ceva ce poate fi numit ciberspațiu, care este de fapt una dintre dimensiunile în care poate fi dus războiul. Ciberspațiul are elemente de bază inseparabile: forțele armate, națiunea și comunitatea internațională. Toate nivelele de comandă și control pot fi atacate și în consecință trebuie să fie apărate. La toate nivelele, omul este cel care are puterea de decizie finală. Acest aspect face din conceptul de „influență" o opțiune și un pericol. Statele moderne se confruntă cu o dilemă. Pe de-o parte, nu au nici o scăpare în fața digitizării. Pe de altă parte, aceste progrese creează noi și serioase vulnerabilități. Conceptele actuale de C2W nu sunt la curent cu dezvoltările recente. Dacă crearea „sistemului sistemelor" este răspunsul, rămâne de văzut. Ciber-terorismul și operațiile informaționale sunt o adevărata problemă. Nu există soluții ușoare. Un prim pas ar fi înțelegerea faptului că riscuri există. Un alt pas constă într-o evaluare atentă a vulnerabilităților. Tehnologia aduce multe foloase dar și o mulțime de greutăți. Există, de asemenea, și numeroase circumstanțe când tehnologia nu este un substitut pentru vărsarea de sânge. Operațiile informaționale pun sub semnul întrebării o serie întreagă de „vechi adevăruri". Ne confruntăm cu conflicte într-o nouă dimensiune. Avem chiar de-a face cu un nou gen de conflict.

ATACUL INFRASTRUCTURII CRITICE

Dr. ADAM COBB

Acest articol consideră Australia ca studiu de caz și caută să răspundă la întrebări ca: unde, cum și de ce infrastructura critică a Australiei ar putea fi supusă riscurilor. Prin examinarea elementelor vitale ale infrastructurii informaționale naționale (NII - *National Information Infrastructure),* cum ar fi sistemele de distribuție a energiei, rețelele de telecomunicații și financiare, este posibil a se măsura gradul de vulnerabilitate al infrastructurii.

Vulnerabilitățile evidente sunt apoi suprapuse peste o selecție de amenințări, prin aceasta efectuându-se o evaluare a riscurilor. Materialul va prezenta la final sugestii pentru viitoare opțiuni politice pentru guvernul australian. Articolul nu pretinde că realizează o trecere în revistă exhaustivă a vulnerabilităților și amenințărilor. Alegerea acestora s-a făcut pe baza literaturii din sursele deschise disponibile.

Tehnologia informației aduce beneficii dar și riscuri. De exemplu, folosirea computerelor legate în rețea în scopuri criminale este un fenomen în creștere care a costat deja Australia milioane de dolari. Un raport din 1997 din mediul guvernamental evidențiază creșterea atât a numărului, dar și a sofisticării atacurilor asupra companiilor australiene în ultimele 18 luni. Cele mai frecvente atacuri au fost asupra sistemelor financiare și datelor confidențiale ale companiilor.

În mod regretabil, riscurile nu se referă doar la crimele electronice. Ele includ tot spectrul, inclusiv accidente și atacuri intenționate. Accidentele includ dezastre naturale, probleme neanticipate (cum a fost problema anului 2000), defecțiuni tehnice și erori ale utilizatorilor.

Amenințările provin din dezinformări, ură/răzbunare (din motive personale sau legate de muncă), crimă, spionaj comercial sau militar, terorism (statal sau nestatal) și războiul informațional. În 1998, zone din Australia și Noua Zeelandă au fost afectate de o severă pană de curent, când punctele cheie ale rețelelor de alimentare cu energie electrică au căzut. Așa cum aceste întâmplări dovedesc, orașele de astăzi sucombă rapid când rețelele lor de energie, telecomunicații și financiare nu mai funcționează corespunzător. În același ton, consecințele unei defecțiuni ale computerelor la 1 ianuarie 2000 ar fi fost dezastruoase.

Totul, de la aparatele video din case și aparatura cu microunde până la sistemul global de poziționare GPS și centralele nucleare din fosta Uniune Sovietică este supus riscului. Fiind o economie avansată, cu o forță de muncă bine educată, cu o infrastructură extensivă, un sector de servicii puternic și în creștere și cu un nivel ridicat al comerțului exterior și al finanțelor, Australia este un exemplu bun al oportunităților și problemelor cu care o națiune din O.E.C.D. se confruntă în era informațională.

Potențiala deteriorare a sistemelor din infrastructura informațională critică privește sectorul privat și cel guvernamental deoarece poate afecta toate elementele vieții sociale care depind de sistemele informaționale. Iată de ce va trebui, în protecția NII, să se prevadă atât riscurile de natură accidentală cât și cele privind deteriorările intenționate ale sistemelor.

O mare parte din literatura despre vulnerabilitățile infrastructurii informaționale s-a scris în urma apariției unui nou subiect în studiile strategice - războiul informațional (R.I.). Acesta reprezintă un domeniu nou și contestat care se referă la abilitatea unei forțe militare de a-și proteja sistemele de informații și cunoștințe proprii în același timp cu atacarea celor ale adversarului. Până în vreme preocuparea privind infrastructura nu este ceva nou pentru strategii militari, noile tehnologii au schimbat felul în care infrastructura funcționează, ducând astfel la necesitatea reexaminării ei într-un context strategic.

R.I. a fost de asemenea asociat cu așa-numita „revoluție în afacerile militare" (RMA - revolution în military affairs). RMA este un concept putemic contestat, iar suporterii lui argumentează că noile aplicații militare ale tehnologiei de vârf asigură forțelor armate moderne progrese revoluționare în domeniile tactic și strategic. În acest nou context, tehnologia stealth, precizia chirurgicală, platformele cu rază mare de acțiune sunt integrate în rețele de senzori, computere și sisteme de comandă și control care permit o viziune foarte largă asupra câmpului de conflict.

Nemaifiind doar un spațiu tridimensional (pământ, aer și apă), câmpul de conflict integrează aceste dimensiuni cu altele două – spațiul și cyberspațiul - unde ducerea războiului depinde de comprimarea timpului și spațiului. RMA se referă și la dezvoltarea structurilor organizaționale care sprijină optimizarea noilor tehnologii, iar de aceea a mai fost numită și „revoluția în afaceri de management".

Această dezvoltare apare la un moment când în lume se petrec evenimente cu o evoluție convergentă.

Prima, violența organizată se concentrează din ce în ce mai mult asupra țintelor civile. În ultimul secol războiul a devenit nu numai apanajul guvernelor și forțelor lor armate, ci și al întregii populații civile. Pe lângă aceasta, spectrul acțiunilor teroriste se concentrează din ce în ce mai mult asupra țintelor „soft".

A doua, puterile statale revoluționare folosesc adesea noile tehnologii în maniere inovative care le oferă, cel puțin la început, un avantaj decisiv în război. Acest secol a însemnat schimbări incredibile ale tehnologiei folosite în scopuri de război, de la artileria trasă de cai la rachete nucleare intercontinentale. Ca o regulă, puterile inovative au avut mai multă imaginație decât cele conservatoare în dezvoltarea doctrinelor și structurilor organizaționale în concordanță cu noile tehnologii. Înainte de izbucnirea celui de al doilea război mondial, generalul Douglas Haig, arhitectul războiului tranșeelor în primul război mondial, declara pompos că viitorul război va fi câștigat încă de la început printr-o

șarjă decisivă de cavalerie. În 1939 exista o egalitate între aliați și germani în ceea ce privește tancurile, aparatura radio și avioanele.

Ceea ce a permis însă germanilor să obțină strălucita serie de victorii din 1939-1940 a fost modul de combinare a acestor tehnologii cu noile concepte tactice. „Blitzkrieg" a combinat tancurile cu aparatura radio, avioanele și infanteria în formațiuni militare (diviziile Panzer) prin utilizarea unor doctrine noi la care Haig și contemporanii săi nu se gândiseră.

A treia, sfârșitul războiului rece, care la fel ca și sfârșitul primului război mondial, a dus la crearea unei perioade de incertitudine la nivel strategic. Deziluziile legate de politicile tradiționale, adâncirea prăpăstiilor dintre diversele entități etnice și rasiale, creșterea mișcărilor împotriva emigrației, insecuritatea locurilor de muncă, speculațiile financiare pe scară largă și incapacitatea politicilor convenționale de a se soluționa aceste probleme sugerează existența unor paralelisme între situația actuală din unele economii dezvoltate și situația din perioada interbelică.

Așa cum spunea E.H. Carr despre perioada 1919-1939, eșecul democrațiilor în a înțelege și depăși excesele distructive ale politicilor care au condus la Marea Criză au dus la apariția unui vid la nivel politic pe care puterile totalitare l-au speculat imediat. Există asemenea paralelisme și la nivel militar și strategic. La fel ca în perioada interbelică, noile tehnologii există în mod curent sub forma „armelor informaționale" dar nimeni nu a formulat încă doctrine sau structuri organizaționale necesare pentru a traduce în practică un „blitzkrieg informațional".

Există astăzi o „revoluție în afacerile militare" în așa multe domenii încât armele, platformele și senzorii militari tradiționali vor deveni mult mai puțin importante decât dependența informațională în creștere a societății civile. Acest lucru are loc într-o epocă în care protecția infrastructurii critice va fi cheia către succesul economic și securitatea națională. Istoria arată că, în

momentele de răscruce din trecut, puterile nemulțumite au luat inițiativa - comercială, militară sau ideologică.

În mediul actual, economic și politic, confuz, cine va căuta noi altemative la vechile dileme va câștiga un avantaj decisiv. Conceptul revoluționar al secolului XXI va scurtcircuita armele tradiționale și se va concentra pe „inima" societății civile - sistemele informaționale de care depinde societatea.

Securitatea națională implică mult mai mult decât apărarea armată. La un nivel minim, apărarea armată este fundamentală pentru supraviețuirea societății. Împingând definiția mai departe, securitatea națională se referă la crearea condițiilor politice, economice, sociale și de mediu înconjurător necesare unei societăți pentru a prospera. În mod evident, un atac asupra NII, de care societățile dezvoltate depind mult, va reprezenta un atac la adresa securității acelei societăți.

În multe cazuri, un asemenea atac va fi de departe mai devastator pentru stabilitatea și capacitatea de funcționare a societății, decât atacul asupra forțelor armate, deoarece el afectează sau distruge elementele de infrastructură cele mai importante pe care societățile modeme se bazează mult.

Ca o consecință, spectrul de conflicte bazate pe informație reprezintă amenințarea cea mai importantă pentru securitatea națională de la dezvoltarea armelor nucleare acum mai bine de 50 de ani în urmă. Ca și armele nucleare, armele bazate pe informație mută centrul strategic de greutate de la forțele militare la atacuri directe asupra țintelor civile. În timp ce folosirea armelor nucleare a deevenit după 1945 ceva de neconceput, este de așteptat ca aceste arme bazate pe informație să fie folosite și să afecteze națiunile dependente de informație.

Conflictul bazat pe informație prevestește un nou tip de conflict, în care asaltul fizic la vedere este înlocuit de infiltrări anonime și omniprezente în societate. Nu se mai poate vorbi despre limite bine precizate, iar aceste infiltrări pot proveni din afară sau din interior. Un asalt informațional asupra diverselor rădăcini ale

societății nu poate fi stăvilit de o birocrație compartimentată care este obișnuită să vehiculeze noțiuni ca divizie de cavalerie sau vase de război.

O abordare holistică, integrată, este acum necesară. Puțini au realizat în trecut că securitatea a devenit acum ceva indivizibil și în viitor va evolua chiar mai mult, în special în contextul realizării securității sistemelor și infrastructurii informaționale de care depinde societatea.

Cu toate că preocuparea pentru securitatea infrastructurii pare a fi apărut din conceptul de RMA, ea nu ar trebui să fie în atenția doar a strategilor militari. Așa cum acest articol încearcă să arate, războiul în accepțiunea sa clasică este doar unul din riscurile la adresa Australiei.

Ce este NII? În contextul acestui articol, NII este compusă din sisteme a căror incapacitate sau distrugere ar avea un impact catastrofal asupra apărării și securității economice a națiunii. Se includ aici: sistemele de telecomunicații, energie electrică, băncile și finanțele, transporturile, de apă etc., atât guvernamentale, cât și private. Din punct de vedere funcțional, ele se pot clasifica astfel:

- *funcții centrale ale statului:* guvern și agenții fundamentale cum ar fi de apărare, intelligence, afaceri externe și comerț, finanțe, asigurări sociale, servicii naționale și regionale de urgență.
- *funcții centrale de utilități:* rețele de alimentare, telecomunicații, rafinării de petrol, sisteme de transport și stocare a gazelor și petrolului, sisteme de trafic și transport (control al traficului aerian, sisteme GPS, instalații meteo) și sisteme de alimentare cu apă.
- *funcțiuni centrale comerciale:* servicii bancare și financiare, mass-media, sisteme de afaceri și rețele de comunicații.

NII se sprijină la bază pe o rețea de telecomunicații și este legată la infrastructura globală (GII -Global Information Infrastructure) prin satelit și cablu submarin. Ea depinde și de o alimentare constantă cu energie electrică și de aceea elementele NII depind

unul de celălalt în funcționare. În următoarea secțiune, înainte de examinarea potențialelor amenințări împotriva acestor sisteme, este efectuată o analiză a vulnerabilităților sistemelor din NII.

Computerele, telecomunicațiile, rețeaua financiară sau comunicațiile militare - zone predispuse unor atacuri informaționale - nu pot funcționa fără energie electrică. Interdependența acestor componente din NII complică eforturile de a le apăra. Complexitatea și interdependența în creștere, în special a infrastructurilor energetice și de comunicații, conduce la o posibilitate crescută ca o problemă minoră și de rutină să creeze efecte în cascadă.

Distribuția de energie în statul New South Wales (NSW) este responsabilitatea unei companii numită TransGrid, a cărei rețea de transmisie are cca. 11500 km și 73 de stații și include generatoare, echipamente de distribuție și 6 centre de comandă locale controlate de la centrul de control de la Carlington, o suburbie a Sydney-ului. Există două surse centrale de alimentare în stat. Una este sistemul pe bază de cărbune de la Hunter Valley, la nord de Sydney.

Celălalt este la Snowy Mountains și cuprinde șase stații principale situate în afară de Canberra la barajele din regiune. Energia produsă este trimisă spre Sydney printr-un singur punct, Yass. Sistemul Hunter asigură, de asemenea, alimentare alternativă pentru Sydney, dar dacă instalațiile de la Snowy Mountains nu funcționează, atunci probabil că sistemul Hunter nu ar putea face față.

Capitala Canberra este deservită de o substație principală care este conectată la doar două alte substații la Yass și Cooma. În Canberra, cele mai multe din agențiile guvernamentale depind de două substații mai mici plasate în oraș. Computerele care deservesc rețeaua de alimentare pot fi accesate print-un număr de rute, incluzând și sistemul de diagnostic folosit de tehnicieni pentru a monitoriza, detecta și rezolva problemele apărute în rețea.

Din acest punct de vedere există vulnerabilități serioase. Prea puține structuri din Departamentul de Apărare, de exemplu, au o sursă altemativă de alimentare cu energie electrică. În mod similar, comandamentele forțelor integrate se află în Sydney și se bazează pe rețeaua de alimentare a orașului, la fel ca și legăturile dintre ele și sediul general din Canberra.

Așa cum a arătat explozia de la rafinăria de la Longford din 1998, sistemele de alimentare cu energie sunt vitale pentru economia națională. Estimări recente au arătat că pierderile generate de incidentul de la Longford se cifrează la aproximativ 1% din PNB. Orașele principale din Australia sunt alimentate cu gaz din două sau trei surse prin intermediul unor conducte extrem de lungi care sunt controlate de computere. Aceste conducte se întind de-a lungul a câtorva mii de kilometri și trec prin locuri nelocuite sau pe sub ocean.

Cu toate acestea, sistemele de calculatoare ce controlează funcționarea acestor conducte nu sunt deloc supravegheate. Accidentul de la Longford ar fi putut la fel de bine să se producă în urmă accesării sistemului SCADA (Supervisory Control and Data Acquisition) ce deservea rafinăria.

Există doi furnizori majori de servicii de telecomunicații în Australia, Optus și Telstra. Telstra dispune de o rețea de cabluri coaxiale, fibre optice, cabluri și fibre submarine, concentratori radio digitali. Există comutatoare dedicate de magistrală în fiecare capitală, plasate într-o ierarhie statică. Rutele sunt testate într-o ordine stabilită, cu cea mai directă dintre ele aleasă la început. Apelurile între orașe pot ocoli hub-urile principale doar dacă toate liniile din hub sunt folosite.

Fiecare hub este legat cu alte capitale prin două rute geografice și fiecare centru de comutare al magistralei are acces către altă capitală. Există un număr important de puncte cheie care dacă sunt atacate, atunci toate comunicațiile terestre între est și vest sunt compromise.

Dacă se adaugă și centrala telefonică de la Camooweal, atunci

întregul centru al continentului ar fi afectat, cu excepția legăturilor directe prin satelit și a legăturilor radio de frecvență înaltă. În aceasta situație, sistemele rămase ar putea fi cu siguranță copleșite de traficul zilnic obișnuit de date și voce.

Australia este de asemenea un nod critic în rețeaua internațională de fibre optice. Apelurile din și către Australia prin cablu submarin și satelit sunt procesate de două instalații din Sydney: centrala de la Paddington și cea a lui Telstra de la Oxford Falls. În afara Australiei, există trei puncte potențiale în Asia unde pot surveni probleme: Japonia, Honk Kong și Singapore. Sud-estul și nord-estul Asiei sunt conectate prin acest coridor submarin.

Legăturile spre exterior trec din Japonia spre SUA, din Singapore spre India și apoi spre Europa. Singurul alt cablu optic submarin care asigură legătura spre SUA și Europa trece prin Australia. În cadrul coridorului asiatic submarin, între nodurile cheie care sunt Japonia și Singapore, Hong Kong-ul este un nod critic. Dacă acesta ar fi afectat, Asia ar fi izolată pe axa de nord-sud. Dacă și Singapore și Japonia ar fi afectate, atunci Australia ar ramâne singura legătura internațională funcțională din zonă. Acest lucru arată clar că Australia este un nod internațional vital.

Rețeaua de comunicații prin satelit cuprinde două sisteme, unul care este parte a sistemului internațional INTELSAT și unul intern (Optus). Atât Optus, cât și Telstra, funcționează ca gateway-uri separate din rețeaua internațională care are aproape 400 de stații în 150 de țări. În plus, Optus și Telstra dispun de stații terestre din INTELSAT, cea de la Telstra fiind o legatură importantă în rețeaua de control internațională a sateliților.

Rețeaua de sateliți Optus, conform unor surse interne, are următoarele tipuri de funcțiuni:

- componentă a sistemelor telefonice Optus și Telstra;
- rețea de management de date pentru bănci;
- monitorizare la distanță a conductelor de gaze și petrol;
- comunicații sol-aer și sisteme de control al traficului aerian;
- semnale de apărare;

- comunicații mobile prin satelit;
- internet;
- servicii radio și TV.

Instalația principală de control a funcționării sateliților Optus este situată la Belrose, o suburbie a Sydney-ului, cu un sistem de back-up la Lockridge. De la Belrose, sateliții pot obține poziția lor pe orbită sau își pot modifica direcția. Este de asemenea posibil să se acceseze și manipuleze semnalele trimise și recepționate de către sateliții Optus și să se monitorizeze traficul de informații prin instalațiile Optus. Nu există criptare pe canalul de control al seriilor A. Oricine care dispune de echipamentul adecvat poate cu ușurință afecta funcționarea seriei A. În mod evident, deci, Belrose este un punct critic.

Banca centrală RBA (Reserve Bank of Australia), este responsabilă pentru stabilitatea de ansamblu a sistemului financiar. Ea este bancherul tuturor băncilor și, în afara de supravegherea băncilor, RBA este responsabilă pentru conturile utilizate la reglementarea obligațiilor interbancare rezultate din sistemul de plăți. Cu alte cuvinte, decontarea cecurilor clienților și transferurile electronice de fonduri sunt responsabilitatea RBA. RBA are în componență sistemul de transfer al informațiilor RITS - Reserve Bank Information Transfer System, care este un sistem de reglementare globală în timp real pentru toate conturile deținute de bancă.

O gamă largă de organizații lucrează împreună cu RBA pentru a asigura desfășurarea corespunzătoare a operațiunilor efectuate. Procesul de decontare implică colectarea informațiilor despre debite și credite și stabilirea pozițiilor între instituții. Reglementarea se referă la „plata sau primirea valorii nete a obligațiunilor stabilite în procesul de decontare".

Procesul de decontare este gestionat de către Asociația Australiană de Decontare a Plăților (APCA - Australian Payments Clearing Association) care este o societate cu răspundere limitată. APCA lucrează împreună cu Societatea de Telecomunicații

Financiare Interbancară (SWIFT - Society for World Wide Interbank Financial Telecomunication) cu sediul în Bruxelles

• Aceasta înseamnă că în fiecare zi băncile australiene efectuează decontările către alte bănci prin intermediul unui computer din Bruxelles care apoi transmite rezultatele la RBA pentru reglarea conturilor deținute de membrii APCA (de exemplu, băncile australiene). Computerul RBA este localizat în Sydney și este legat online cu filialele RBA din toate capitalele.

Băncile au doar 45 de minute pentru procesul de decontare și reglare în fiecare zi lucrătoare - de la 8.00 la 8.45. Rămân astfel 15 minute înainte de 9.00 pentru RBA ca să intervină, dacă este necesar, în cazurile în care o bancă nu-și poate onora angajamentele rezultate din procesul de decontare. 45 de minute nu este mult pentru efectuarea unor intervenții în caz că ceva nu merge cum trebuie. Sistemul bancar intern nu poate supraviețui mai mult de câteva zile dacă acest sistem delicat este afectat.

În multe situații în cazul tranzacțiilor electronice interne, membrii rețelei cad de acord asupra obligațiilor bilaterale și notifică apoi această RBA. Ca o consecință, toate băncile importante au centre de procesare a datelor conectate unul la celălalt și la sistemul principal al RBA. Din motive de „eficiență", centrele de procesare a datelor sunt doar câteva.

Un asemenea centralism a cauzat deja probleme. De exemplu, în 1990 funcționarea centrului de date al băncii ANZ din Melboume a fost întreruptă când linia de alimentare cu energie a unui tramvai a intrat în contact cu acoperișul băncii ca urmare a unui accident.

Multe alte tranzacții importante se fac prin intermediul computerului RBA. Acestea includ plățile pe care guvernul le face către 600 de instituții financiare, care la rândul lor distribuie aceste plăți în conturile a milioane de australieni - funcționari publici, membrii forțelor armate, beneficiarii de servicii sociale etc. În 1993, acest sistem a efectuat 3 milioane de tranzații pe zi.

Aceasta reprezintă un punct slab cheie al sistemului. Dacă,

spre exemplu, în cazul apariției unui conflict major, un adversar ar afecta sistemul de plăți guvernamental către forțele armate și familiile lor, atunci moralul acestora și al societății în general ar putea fi serios afectat. Acest mod de distrugere a fost evidențiat în trecut cu grave consecințe politice.

Criza bugetului federal din 1975 s-a transformat rapid într-o criză constituțională când guvernul a avut de înfruntat un Senat ostil, ceea ce ar fi condus la imposibilitatea efectuării plăților pentru armată și nu numai. Cu toate plățile guvernamentale făcute printr-un singur computer, securitatea financiară a milioane de australieni, precum și stabilitatea națională economică și politică sunt puse serios în primejdie.

Evaluarea riscurilor este un proces care suprapune vulnerabilitățile existente peste amenințările posibile pentru a determina ceea ce este mai probabil a se produce. Ca în multe țări din OECD, infrastructura informațională națională a Australiei este supusă unor pericole intenționate sau nu. Accidentele includ dezastre naturale, probleme neanticipate (cum ar fi problema anului 2000), defecțiuni tehnice sau greșeli ale utilizatorilor. Amenințările includ dezinformări, ură / răzbunare (personală sau legata de muncă), crimă, spionaj economic sau militar, terorism de nivel statal sau nestatal și războiul informațional.

Amenințările, cum ar fi terorismul, nu sunt neapărat mai periculoase decât cele accidentale, dacă probabilitatea de desfășurare a unui act terorist este foarte scăzută. În anumite cazuri, probabilitatea de desfășurare a unui eveniment este redusă dar consecințele sunt atât de grave încât acestei amenințări îi este acordată o prioritate mare.

Două lucruri trebuie precizate în acest context. Consecințele unei defecțiuni apărute în NII sunt, fără îndoială, foarte grave. De aceea vor trebui luate măsuri indiferent de evaluările probabilității amenințărilor. O dată ce probabilitatea este luată în considerare, este clar care riscuri necesită cele mai urgente acțiuni. Al doilea, în anumite cazuri, există o combinație de niveluri înalte de

vulnerabilitate, o probabilitate mare de producere a unui eveniment și consecințe asociate severe. Oriunde există o suprapunere a acestor trei factori, există o ierarhie a amenințărilor.

Evaluarea riscurilor efectuată în acest articol sugerează o ierarhie a amenințărilor cu care se confruntă infrastructura critică a Australiei. Într-o ordine descrescătoare a probabilității și consecințelor asupra securității naționale, avuției și poziției internaționale a Australiei, ele sunt:

- problema anului 2000;
- terorismul informațional;
- activități criminale majore;
- dezastre naturale;
- terorism statal sau nestatal;
- războiul informațional asupra sistemelor civile;
- războiul informațional asupra sistemelor militare.

Cel mai mare risc în anul 2000, asupra NII, părea a proveni de la o „amenințare" neintenționată, dar cu toate acestea foarte severă. Incompatibilitatea computerelor la trecerea în anul 2000, care putea afecta computerele de pretutindeni, precum și cipurile integrate. Căderile de sisteme datorate Y2K au impact nu doar asupra computerelor și rețelelor individuale, ci efectele lor pot fi la fel de devastatoare ca și un atac criminal concentrat. În mod similar, un colaps în cascadă propagat de la sistemele cu probleme, la întreaga rețea, pot amenința sisteme care au fost „imunizate" la Y2K.

Y2K nu accentuează doar vulnerabilitățile depistate în NII, dar crește și probabilitatea lor de apariție. Consecințele unor defecțiuni multiple a unor sisteme interdependente pot paraliza națiunea mai grav decât ar putea face un atac militar.

În esență, problema constă în faptul că multe echipamente hardware și programe software au fost realizate de o astfel de manieră încât folosesc data calendaristică pe două cifre. Data pe două cifre se folosește în milioane de fișiere de date, în milioane de aplicații și în o mare varietate de sisteme hardware și sisteme de operare.

Problema afectează cel mai mult computerele și software-ul din echipamentele electronice. Măsurile de corecție includ inspecția, evaluarea, modificarea și testarea a milioane de linii de cod, ceea ce este consumator de timp și resurse materiale. O mare parte din gravitatea acestei probleme constă în timpul scurt ce a rămas la dispoziție și la gravitatea posibilelor efecte.

La 1 ianuarie 2000 orice computer care nu a fost pregătit va prezenta dificultăți în funcționare. Acest lucru poate avea efecte deosebit de grave dacă se are în vedere că este suficientă o singură „verigă" care nu prezintă conformitate cu anul 2000 pentru a se afecta rețele întregi. Există deci un risc deosebit de ridicat ca infrastructuri care se bazează pe computere legate în rețea să se confrunte cu defecțiuni serioase, dacă nu chiar catastrofice. Din cauză că toate se întâmplă simultan în întreaga țară, este imposibil să se prevadă impactul global și de aceea acesta este fără precedent.

Nu doar infrastructurile civile cheie depind de computere și rețele. La o conferință recentă desfășurată la Canberra, autorul articolului de față l-a întrebat pe comandantul forțelor aeriene americane, gen. Michael Ryan, dacă forțele nucleare strategice ale SUA sunt complet protejate împotriva Y2K.

Răspunsul lui a dat asigurări că toate sistemele sunt conforme cu cerințele de trecere la anul 2000, însă mass-media internațională pune la îndoială capacitatea Rusiei și fostelor republici sovietice de a se adresa amenințărilor Y2K. De exemplu, *Sunday Times* a raportat recent că surse occidentale de intelligence au avertizat liderii politici că ar putea exista un „Cernobâl gigant" dacă problemele legate de Y2K, la nivelul sistemelor nucleare militare și civile din fosta Uniune Sovietică, nu sunt rezolvate. Același ziar îl citează pe consilierul președintelui Bill Clinton pe probleme de Y2K, John Koskinen, care a sugerat ca sistemele SUA ar putea să nu fie așa de sigure precum declară generalul Ryan. Preocupare și îngrijorare există nu numai la nivel militar. Bursa de valori australiană a cheltuit 12 milioane de dolari pentru a-și verifica și

imuniza sistemele împotriva „bug-ului mileniului" și coordonează companiile australiene în domeniu.

După ce s-a analizat amenințarea neintenționată care se prezintă sub forma problemei Y2K, se poate trece în continuare la considerarea amenințărilor intenționate. Nici una din vulnerabilitățile discutate anterior nu ar fi importante dacă nu ar exista o amenințare semnificativă la adresa Australiei. Trebuie de asemenea reamintit că trebuie să existe patru elemente centrale de urmărit în identificarea amenințărilor probabile: motiv, oportunitate, capabilitate și hotarâre.

NII poate fi atacată în multe moduri. Există în prezent în literatura despre războiul informațional multe discuții foarte aprinse despre un „Pearl Harbour electronic". Atacurile asupra NII nu sunt așa ușor de organizat precum sugerează unele comentarii, dar în orice caz sunt mai ușor de organizat decât s-ar putea imagina, acest lucru depinzând de țintă și de amploarea atacului.

Atacuri de masă asupra NII nu sunt posibile fără o planificare și intelligence la nivel de detaliu și fără personal foarte calificat. Numărul mare de sisteme și gradul de interconectare între acestea reprezintă chiar o formă de securitate deoarece nu este posibil de a face nefuncționale aceste sisteme fără cunoștinte detaliate despre slăbiciunile și poziția nodurilor critice din interiorul acestora. Doar o lovitură bine sincronizată și coordonată ar putea avea după aceea un efect total.

Așa cum a fost prezentat anterior, consecințele unui atac ar putea crește dacă caracteristicile de redundanță ale sistemului au fost degradate datorită imperativelor comerciale de reducere a costurilor, centralizare a nodurilor critice, reducere a operațiunilor de întreținere și folosire a soluțiilor hardware/software comerciale și comune.

Cu toate acestea, un atac în masă este puțin probabil. Chiar dacă elemente de planificare și intelligence sunt folosite pentru atacuri informaționale de mare amploare, aceste atacuri trebuie

să fie declanșate de entități statale și doar împreună cu alte forme de violență organizată.

Oricum, în cazul unei acțiuni militare, atacarea elementelor centrale ale NII și centrilor informaționali ar duce la surprindere strategică și ar favoriza desfășurarea în continuare a războiului convențional.

Aceasta nu înseamnă că Australia este invulnerabilă. Dimpotrivă, un atac asupra nodurilor critice ar putea duce la o reacție în lanț care ar avea efecte devastatoare pentru societate. Un atac s-ar putea concentra cel mai probabil asupra unuia sau a două sisteme cheie.

Chiar defecțiuni de mică amploare ale sistemelor cheie, fără planuri adecvate de restabilire, ar putea afecta în mod serios guvernul, sectorul comercial și societatea în ansamblul ei. Pe lângă atacul fizic, cea mai la îndemână formă de atac este interzicerea serviciului. Aceasta nu necesită penetrarea sistemelor informaționale (pentru care sunt necesare parole sau spargeri ale codurilor sursă), ci mai degrabă supraîncărcarea nodurilor cheie din exterior (care este o formă de sufocare a sistemelor, prin aceasta împiedicându-se funcționarea sistemului și afectând operațiunile sale interne.

Tehnici de info-terorism

- atacuri de interzicere a serviciilor;
- „aranjarea" hardware-ului și software-ului (înseamnă realizarea unor inserții speciale în microcipuri sau în cod la momentul fabricării / programării pentru a permite accesul ulterior neautorizat);
- intruziuni în sistem (prin „spargerea" parolelor sau exploatarea slăbiciunilor sistemului de operare);
- atacuri cu viruși de computer (bombe logice, cai troieni, viermi);
- atacuri fizice (incluzând bombe cu impulsuri electromagnetice);

- bruiaj și alte tehnici de război electronic;
- interceptia informațiilor (interceptia radiației Van Eck).

Cea mai sofisticată (și în consecință cea mai dificilă) formă de atac este penetrarea sistemului. Obținerea accesului la sistem poate fi o operațiune dificilă și de durată. Sistemele de mare securitate, cum ar fi cele utilizate în scopuri militare sau bancare, sunt izolate de sistemele exterioare sau protejate de măsuri de securitate cum ar fi firewall-urile. Este dificil, dacă nu chiar imposibil, să se aibă acces la aceste sisteme din exterior (doar dacă cineva din interior nu a „aranjat" sistemul sau a „spart" firewall-ul).

Prin afectarea legăturilor sistemului se pierd toate avantajele legării în rețea, cum ar fi conectivitatea multiutilizator. Uneori, acest cost este prea mare și, surprinzător, într-un număr destul de mare de cazuri, sistemele de importanță critică sunt legate cu alte sisteme care pot fi penetrate din exterior.

Problemele discutate anterior devin și mai complicate în cazul infoterorismului, a doua sursă de amenințări pentru Australia după Y2K. Interesele teroriștilor sunt bine servite de tehnologia informației. Costuri reduse, dificultăți în identificarea atacurilor și originii lor, precum și potențialul haos ce s-ar crea în mediul guvernamental și în societate în ansamblu, oferă oportunități deosebite pentru teroriști.

Aceștia vor fi întotdeauna atrași de faptul că noțiunile tradiționale de descurajare vor deveni din ce în ce mai desuete în contextul operațiunilor informaționale, în care un atacator (aflat poate chiar în interiorul țării atacate) poate lansa atacuri de pe un computer mobil, mascându-și sau schimbându-și identitatea.

Olimpiada reprezintă o oportunitate deosebită pentru un terorist în viitorul apropiat, cel puțin pentru faptul că mai multe evenimente sportive de acestă anvergură desfășurate în trecut inclusiv Munchen și Atlanta, au fost marcate de acte de terorism. Instituțiile de aplicare a legii se concentrează pe securitatea fizică și nu par preocupate de chestiuni ca cybersecuritatea. Un atac

poate fi declanșat împotriva Australiei sau, la fel de bine, împotriva unei alte țări participante la spectacolul televizat care se va desfășura, datorită spectrului larg de ținte și oportunități ce apar în acest context. Având în vedere „spaima" creată de problema anului 2000, este posibil ca sub această acoperire să fie inițiate acte pe scară redusă sau pe scară largă care ar putea compromite jocurile și afecta reputația Australiei.

O sursă guvernamentală australiană care a dorit să-și păstreze anonimatul a declarat în *Australian Financial Review* că guvernul federal nu a respectat în totalitate promisiunea de a dezvolta și implementa o strategie de securitate pentru desfășurarea jocurilor. Sursa respectivă a avertizat că Australia nu este pregătită pentru contracararea terorismului olimpic și că acte semnificative de violență pot apare.

Un exemplu interesant de terorist bine educat, motivat și fără remușcări și care ar fi folosit noua tehnologie a informației pentru a obține efecte sporite il reprezintă „Unabomber" (pe numele lui adevărat Theodore Kaczynski, care și-a câștigat „faima" în SUA timp de 17 ani prin trimiterea bombelor în colete care au ucis un număr mare de persoane).

El a publicat un manifest în care explica ceea ce l-a determinat să facă aceste gesturi. A fost arestat până la urmă în 1996, în urmă unui denunț. Cu resurse suficiente încât să achiziționeze un computer și un modem și cu puternice resentimente împotriva societății, un terorist de factura „Unabomber" ar putea produce pagube considerabile.

Dacă un asemenea terorist ar rămâne nedescoperit, așa cum a rămas Unabomber, implicațiile sociale ale actelor sale ar fi majore. Un asemenea terorist ar fi capabil de descoperirea nodurilor critice și de ascunderea identității sale pentru a avea acces la coduri și parole, prin aceasta câștigând acces la sistemele vitale pentru funcționarea societății.

Într-o perioadă a insecurității locurilor de muncă, a reducerilor alocațiilor bugetare în multe domenii (este de amintit că Unabomber era un absolvent de matematică de la Harvard)

posibilitatea de a exista teroriști este ridicată în țări ca Australia și SUA mai mult ca oricând, în condițiile în care tot mai multe persoane au acces la sistemele vitale din NII și la tehnicile de atacare a acestora. Efectele acestor tehnici sunt foarte greu de imaginat dacă teroristul tip Unabomber se întâmplă să fie managerul unor sisteme critice.

A treia zonă a operațiunilor informaționale este reprezentată de crimă. Criminalii și grupurile criminale organizate au sesizat rapid oportunitatea oferită de noile tehnologii ale comunicației și de nivelul de răspândire a acestora în societate. Un expert în crima organizată a declarat în *The Australian* că, cartelele crimei sunt deja cu cel puțin doi ani în față în ceea ce privește tehnologia sofisticată.

Din cele patru domenii de potențiale amenințări identificate anterior, crima este cea mai des întâlnită ca aplicare a tehnicilor și strategiilor de operațiuni informaționale. În cadrul operațiunilor informaționale, tehnicile pentru atacarea unui sistem de control al traficului aerian sunt același cu cele utilizate la atacarea unei bănci. Ca o consecință, statisticile privind cybercrima sunt foarte folositoare, deoarece nu există dovezi clare privitoare la războiul informațional sau acțiunile teroriste.

Biroul de evaluare a crimelor strategice *(OSCA* -Office for Strategic Crime Assessment) din cadrul Departamentului procurorului general al Australiei a desfășurat un studiu care a cuprins 500 de companii, departamente guvernamentale și alte organizații mari și care a urmărit să investigheze tipul, modul de desfășurare și frecvența atacurilor informaționale pe care aceste structuri le-au suferit. Rezultatele care s-au obținut sugerează ceea ce se poate aștepta în viitor de la grupările teroriste și competitorii militari.

Studiul arată ca agențiile australiene de aplicare a legii au raportat creșteri spectaculoase atât a numărului, cât și a gradului de sofisticare, a atacurilor exterioare asupra companiilor australiene în ultimele 18 luni. Sistemele financiare și datele confidențiale ale companiilor au fost două din cele mai favorite ținte ale atacurilor. Motivațiile atacurilor au fost: extorcarea și

terorismul (11%), spionajul (26%), câștiguri financiare (10%), producerea de deteriorări (4%) și curiozitate (49%). Cea mai mare parte din atacuri a provenit din interior (angajați etc.) dar creșterea atacurilor provenite din exterior este însemnată.

Rezultatele studiului australian sunt similare cu cele obținute în urma studiilor internaționale. Atacatorii din exterior au folosit Internetul (25%), remote dial-in (16%) și alte „rute" (19%). Un oficial al unei bănci importante a estimat că pierderile suferite în urma atacurilor informaționale depășesc 500000$.

În această perioadă Australia nu se confruntă cu amenințări provenite de la alte state din regiune. Acest fapt reprezintă premisa de la care s-au alcătuit planurile strategice de apărare și nu există motive imediate pentru schimbări. Tendințele pe termen lung din regiune ridică însă semne de întrebare. O serie de țări s-au confruntat deja cu dificultăți financiare și economice de neconceput cu câțiva ani în urmă.

Operațiile informaționale oferă mari avantaje țărilor în dezvoltare. Mai puțin dependente de sisteme informaționale în desfășurarea activităților de zi cu zi, vulnerabilitatea lor la atacuri este mai scazută. Având în vedere disponibilitatea pe scară largă a informațiilor despre tehnicile folosite în operațiile informaționale și costurile relativ scăzute de achiziție a acestor tehnici, nu încape îndoială că operațiile informaționale reprezintă o opțiune atractivă.

Deoarece oferă și posibilitatea acționării sub anonimat, operațiile informaționale sunt compatibile pe deplin cu operațiunile sub acoperire. În contextul creșterii tensiunilor regionale, chiar cel mai puțin dezvoltate națiuni pot dezvolta motive, oportunități, capabilități de a lansa atacuri informaționale.

Operațiile informaționale par a oferi statelor în curs de dezvoltare posibilitatea de a contracara asimetriile de putere dintre ele și țările dezvoltate. Acum aceste lucruri par doar probabile, dar cine știe ce se va întâmpla după în anul 2010?

Operațiile informaționale nu sunt o opțiune la fel de atractivă în cazul structurilor putemic dependente una de cealaltă. Consecințele unui atac asupra sistemului financiar al statului vecin

se pot răsfrânge asupra atacatorului dacă acesta depinde de sistemul în cauză.

În literatura pe marginea operațiilor informaționale se sugerează că folosirea acestora se face izolat de acțiunile militare. Care ar fi scopul unui atac pe scară largă asupra NII a Australiei, dacă nu preludiul unei invazii? Utilizate ca prime lovituri într-un conflict major, operațiile informaționale ar fi un element de surpriză cheie care ar putea afecta sistemele centrale. Acest lucru ridică o serie de întrebări privind răspunsul adecvat și controlul escaladării conflictului. Este un asalt asupra infrastructurii financiare un act de război, presupunând ca atacatorul a fost identificat? Care ar trebui să fie riposta?

Până recent, a fost dificil să se cuprindă toate aspectele securității informaționale deoarece acest lucru a fost perceput ca ceva tehnic. Însă dependența societății de sistemele informaționale cere ca securității informaționale să-i fie acordată mai multă atenție. Deoarece Australia are multe avantaje din statutul său de economie informațională, răspunsul trebuie să prezinte mai multe aspecte și trebuie să se concentreze asupra exploatării oportunităților ridicate de era informațională, precum și asupra căutării celei mai complete protecții.

Există patru propuneri principale care pot fi cu ușurință implementate și cu costuri minime. Prima este criptarea. Acest lucru ridică destule controverse în mediul guvernamental, deoarece nu este de dorit ca tehnologia să ajungă „pe mâini nepotrivite". Criptarea oferă un nivel de securitate pentru toți utilizatorii ce o folosesc și teama pe care o încearcă unii este că creșterea dificultății de a sparge cheile criptografice va duce la creșterea dificultăților de a afla ceea ce zic oamenii. Fără a oferi prea multe amănunte, este suficient de spus că criptarea oferă protecție sistemelor informaționale.

A doua, când cineva se gândește la securitatea informațională spune imediat firewall. Cu toate acestea studiile, precum și opiniile experților, arată că în multe cazuri cele mai importante măsuri de protecție încep cu proceduri simple la birouri și acasă, cum ar fi

ascunderea parolelor. Ceea ce este cu adevărat de dorit este o schimbare la nivelul „culturii de birou", în sensul respectării cerințelor privind securitatea informațiilor. Cea mai bună cale de a realiza securitatea informațiilor la nivelul corporațiilor este desfășurarea unor programe educative și de instruire.

A treia, în viitorul imediat planurile companiilor trebuie să fie dezvoltate pentru a ține cont de eventualitatea unui atac informațional. De exemplu, dacă centrala telefonică de care depind comunicațiile terestre ale Departamentului de Apărare este atacată, are departamentul un plan care stabilește prioritățile de comunicații cu ajutorul sistemelor de rezervă? Dacă, în plus, rețeaua de alimentare cu energie electrică este atinsă și pune în pericol sistemele de apărare?

Există un plan care stabilește prioritățile organizației astfel încât funcționarea sa să nu fie prea mult afectată dacă sistemele centrale de energie și comunicații sunt atinse? Aceste întrebări pot fi puse și în cazul băncilor și altor elemente vitale ale NII. Mai degrabă decât a dispune de soluții la problemele anterior arătate, pare a fi mai oportun de desfășurat planuri la nivel organizațional. Acest lucru, totuși, nu exclude cooperarea și coordonarea, pe plan local și internațional, ca o practică foarte utilă în protejarea NII.

În final, ar trebui înființată o Agenție de protecție a infrastructurii naționale în cadrul cabinetului primului ministru. Aceasta ar trebui să cuprindă un consiliu, un centru de avertizare și un secretariat. Rolul consiliului ar fi să coordoneze activitatea întregii agenții și să facă recomandări cabinetului pentru a asigura securitatea și buna funcționare a infrastructurii naționale.

Consiliul ar trebui să aibă membri din ministerele și companiile implicate în funcționarea infrastructurii. Centrul de avertizare, partea centrală a organizației, ar trebui să fie un sistem de monitorizare pe scară largă care detectează și urmărește orice neregularitate în funcționarea infrastructurii. Secretariatul ar trebui să aibă un centru de conducere, membrii săi putând proveni din agențiile implicate în protecția infrastructurii.

Există o legătură între diversitate și conectivitate în sistemele informaționale. Diversitatea în sistemele informaționale induce securitate, dar complică monitorizarea în interiorul sistemului și de-a lungul interconexiunilor între sisteme. Deoarece atacurile informaționale foarte probabil vor fi anonime sau vor proveni de la surse cu o identitate neclară, funcția de monitorizare trebuie să fie una esențială. Agenția trebuie să testeze și să monitorizeze sistemele existente, pe baze anonime, pentru a se descoperi orice activitate suspectă. Odată ce este descoperită o neregularitate, agenția notifică utilizatorii și dezvoltă planuri de contracarare.

Nevoia pentru o asemenea organizație este recunoscută de oficialii responsabili pentru siguranța NII din cadrul departamentului procurorului general care declara că, la un nivel minim, Australia are nevoie de *„o bază de date despre incidentele informaționale care au avut loc... altfel va fi foarte greu de a ști dacă securitatea este la un nivel corespunzător. Similar, dacă informațiile sunt distribuite, avem nevoie de un mecanism de informare a organizațiilor cu privire la ultimele amenințări și tehnici de securitate".*

Supravegherea activității agenției ar trebui să fie misiunea unei comisii cuprinzând reprezentanți din mediul de afaceri și din agențiile guvernamentale și al cărei rol este de a face recomandări guvernului cu privire la strategiile de urmărit. Nu este necesar, și nici de preferat, să se creeze un minister nou pentru așa ceva ci, mai degrabă, ar trebui ca această responsabilitate să fie acordată unui portofoliu existent.

La o primă vedere, această inițiativă nu ar stârni prea mult entuziasm.

Totuși, tendințele existente dovedesc că cele mai multe organizații aflate la partea centrală a NII realizează că actul de coordonare va fi vital atât pentru interesele lor particulare, cât și pentru cele de grup, și acest lucru pentru că siguranța unora nu a fost nicicând mai dependentă ca acum de a celorlalți. Studiul la care s-a făcut referire anterior este convingător, deoarece se bazează pe exemple atât din domeniul guvernamental, cât și privat,

și demonstrează că cele două zone ale societații sunt dispuse să lucreze împreună în acest domeniu de importanță vitală.

CONCLUZII

Ca un exemplu de stat tipic din O.E.C.D., Australia este vulnerabilă la atacurile informaționale. Există multe noduri cheie în NII care ar putea fi exploatate de către agresori. Interdependența dintre sisteme, cum ar fi cele de telecomunicații, energie și rețele financiare, precum și dependența sistemelor informaționale ce funcționează în societate, prezintă noi provocări pentru autoritățile guvernamentale și organismele private. Criminalii și sindicatele crimei organizate exploatează deja din ce în ce mai mult slabiciunile din NII.

Există motive să se creadă că amenințările posibile la adresa NII există și ele vor crește în intensitate pe măsură ce teroriștii și statele agresive caută să exploateze noile tehnologii. Cu toate acestea, există o serie de strategii care pot fi adoptate pentru protecție.

Unele sunt soluții simple, altele necesită o coordonare dar cu costuri de implementare destul de reduse. Elaborarea unei strategii cuprinzătoare pentru Australia prin care se caută realizarea protecției necesare, pe lângă creșterea robustetii NII, reprezintă un bun punct de plecare pentru funcționarea economiei și societății în ansamblu în noul mileniu.

Există câteva lecții importante desprinse din cazul Australiei pentru economiile avansate, cum ar fi cele din Europa Occidentală și America de Nord. Dependența infrastructurilor critice de computerele legate în rețea prezintă o gamă largă de provocări pentru strategii secolului XXI.

Războiul informațional oferă imaginea unor grupuri dispersate de teroriști care beneficiază de oportunități de a ataca și de a afecta (iar în cazul extrem de a distruge) fundamentele societății modeme. Trebuie luate in permanență măsuri și nu

Războiul informațional oferă imaginea unor grupuri dispersate de teroriști care beneficiază de oportunități de a ataca și de a afecta (iar în cazul extrem de a distruge) fundamentele societății modeme. Trebuie luate in permanență măsuri si nu

RĂZBOIUL NEOCORTICAL UN CONCEPT PENTRU VIITOR

HENRIK FRIMAN*

În orice discuție privitoare la războiul informațional percepția este elementul central și factorul cheie al succesului. În acest material voi încerca să stabilesc dacă informația sau percepția reprezintă principalul obiect al războiului informațional. Cea mai mare parte a literaturii consacrate războiului informațional face puține referințe la ideea de „război al percepțiilor".

În acest text vom vorbi despre existența a ceea ce s-ar putea numi război al percepțiilor și vom încerca să descriem acest fenomen. Vom argumenta faptul că războiul percepțiilor nu este un fenomen nou, dar de cele mai multe ori a fost luat în discuție ca parte a altor concepte de război.

Făcând din războiul percepțiilor obiect de studiu și dezvăluindu-l, într-un anumit sens, sperăm să dăm o mai mare valoare conceptului. Nu poate fi negat faptul că suntem în mod constant obiecte ale atacurilor de percepție, dar ce face din ele un război al percepțiilor? Acest material se dorește a constitui un prim inventar al problemelor dintr-o zonă care are nevoie a fi mai bine cercetată.

Războiul tradițional este o afacere de mare risc în care vieți omenești sunt sacrificate pentru atingerea anumitor scopuri. Dintr-o perspectivă umanistă, omul politic sau cadrul militar de conducere a trebuit să decidă întotdeauna dacă scopurile pot fi atinse fără a

* Colegiul suedez de apărare națională, Departamentul de studii operaționale.

face apel la mașinăria infernală a războiului. Clausewitz ne-a învățat că scopurile unei lupte nu înseamnă întotdeauna distrugerea forțelor inamicului și că acestea pot fi atinse fără ca lupta să aibă loc.

În cadrul celor mai multe forme de război, iluzia victoriei sau a înfrângerii e definitorie, nici unul din participanți nedorind să piardă. E vorba de modul în care participanții percep evenimentele în contextul situației în care se află. Războiul percepțiilor este acel concept care permite să se creeze evenimente care produc iluzii tuturor că sunt învingători, în felul lor. Este vorba de o luptă dusă la nivelul mentalului comandanților.

Argumentăm în acest material faptul că ceea ce au în comun confruntarile din trecut cu cele din viitor este încercarea de a impune voința asupra părții adverse. În țările dezvoltate violența fizică nu e acceptată și societatea previne manifestarea acesteia prin toate pârghiile de care dispune.

În acest context nu este credibil să previi, pe de o parte, violența în societate și pe de altă parte, să creezi forțe pentru a face față diverselor conflicte. Mai este mult de făcut până să vedem o lume fără violență și pentru acest lucru trebuie să vedem războiul percepțiilor ca un complement al altor forme de luptă. Ideea centrală este că cel care ia decizii va evita violența utilizând, pe cât posibil, alte mijloace pentru a-și atinge scopurile. Unei astfel de idei i se poate argumenta că atacul asupra psihicului uman, cum ar fi spălarea creierului, nu este un lucru etic și această percepție a atacului poate avea loc în secret, fără ca o declarație de război să fie făcută. Amândouă argumentele se susțin și nu le putem nega relevanța. Totuși, în acest material nu vom apăra nici o poziție privind problemele de etică, ci ne vom concentra asupra descrierii războiului percepțiilor fără a aborda și aceste chestiuni.

Războiul poate fi văzut ca o luptă între entități aflate în competiție sau ca operații militare între mai mulți adversari. Scopul este de a slăbi sau a distruge adversarul. Războiul poate fi surprins în multe forme, ca război de intervenție, ca război de opinie sau

război național [35]. În literatură, același interes poate fi acordat diferitelor forme de intervenție, de exemplu, aeriană, biologică, chimică sau război informațional. Handel [36] afirma că definiția războiului e o problemă de nivel al analizei.

O parte a confuziei poate fi explicată prin diferențele existente la nivelul grupurilor de lucru și a definițiilor. Ceea ce e asemănător pentru toate descrierile este faptul că încercăm conștient să ne atingem scopurile utilizând forța.

Războiul percepțiilor nu este același lucru cu războiul informațional, deși există multe asemănări. Cu câțiva ani în urmă am încercat să descriem diferitele perspective ale conceptului de „război informațional" (Friman, Sjöstedt and Wik, 1996) [37].

Concluzia acestui studiu a fost că filosofiile din spatele conceptului de război informațional nu reprezintă un lucru nou, doar că noile tehnologii dau noi posibilități. Un exemplu este atacul unei surse de informații folosind informația ca armă. În discuțiile de până acum s-a accentuat în special aspectul tehnologic al războiului informațional, care asigură soluții pentru a realiza controlul asupra fluxurilor informaționale care înconjoară crizele.

Concepte sau tehnici de genul războiului de comandă-control, a războiului bazat pe informații, a războiului electronic, a războiului psihologic, a războiului electronic, a războiului hackerilor, a războiului informațiilor economice și a războiului din spațiul realității virtuale au fost inventate pentru a da diferite explicații conceptului de război informațional [38]. Alte concepte sunt propaganda, războiul de inducere în eroare și dezinformarea. Elementul central al acestor concepte este lupta pentru a controla informația și utilizarea ei pentru a crea intenționat anumite efecte.

Experiențele au arătat că e dificil să controlezi producerea unei activități de război informațional. Analizele au arătat că

[35] H. Jomini, *The Art of War*, Greenhill Books, London, 1992.

[36] M. Handel, *Masters of War: Classical Strategic Thought*, 2 ed. Frank Cass, London, 1996.

[37] Într-un studiu la Swedish Institute of International Affairs.

[38] Libicki, *What Is information Warfare?*, National Defense University, Washington, 1995.

aceiași indivizi acționează în mod diferit în circumstanțe diferite având aceeași informație, ceea ce indică faptul că informația disponibilă nu explică prin ea însăși realizarea unei operații informaționale și că problema e mult mai complexă decât aceea a unei relații stricte dintre informație și realizare.

O explicație a acestei complexități constă în faptul că fiecare individ creează „imagini" diferite în cazul aceleiași situații, care depind de starea emoțională a acestuia la momentul respectiv.

Presupunerile privind efectele în războiul informațional sunt construite pe legea numărului mare pe care îl deține în statistici, similar abordărilor unor afaceri generale. Produsul așteptat este măsurat, dar nu oferă nici o garanție că grupul va realiza în realitate, aceleași activități. În statistică interesul constă în a prevedea urmările la nivelul unui grup numeros de oameni și e puțin hazardat a pretinde a putea prezice actele fiecărui individ în parte.

În sociologie, actele anumitor indivizi, așa-numiții „lideri", vor influența acțiunea altora, a celor care le împărtășesc convingerile sau care dintr-un motiv sau altul depind de ei. Pentru a crea o activitate eficientă de război informațional ar trebui să ne concentrăm asupra liderilor care (in)direct îi afecta pe cei care-i urmează.

Credem că cel care comandă, care ia decizii este principalul punct de concentrare a activităților informaționale. „Imaginea" situației e esențială pentru viitoarele acțiuni ale grupului sau organizației și de aceea „lupta" informațională este, de fapt, un război al percepțiilor, o creație a acestei imagini.

Publicul va fi influențat de declarațiile liderilor și indirect afectat de credințele celui care comandă. Această perspectivă se apropie de propagandă, dar diferă din punct de vedere al obiectivelor. În cazul războiului percepțiilor obiectivul este un anumit element individual, în timp ce în cazul propagandei obiectivul îl constituie opinia publică.

Mao Tse Tung (*On the protracted war*, 1938) spunea odată că *„pentru a câștiga trebuie să încercăm să pecetluim urechile și*

ochii adversarului, să-l orbim și să-l surzim și pentru a crea confuzie în mintea comandanților adverși si să-i aducem în pragul nebuniei". Declarația sa omagiază ceea ce noi numim războiul percepțiilor. Până acum, au fost publicate foarte puține articole care să abordeze explicit problema războiului percepțiilor.

Una din primele referințe este lucrarea lui Glenn și Peterson [39], în care războiul percepției este explicit discutat în contextul rolului psihologiei în războiul informațional, ceea ce pare a fi un mod des întâlnit pentru a privi problema percepției. Problema percepției e, în mod tradițional, văzută că parte a războiului psihologic, în termeni de percepție a managementului.

Credem că, pentru a avea succes, problema percepției e centrală și nu doar în contextul războiului psihologic sau informațional, și că războiul percepției merită să constituie un element de sine stătător și nu doar o componentă a altor concepte. În viitor, putem avea de-a face cu un război al percepției. De aceea studiul acestui tip de război este foarte relevant pentru viitoarele abordări.

Conceptele războiului percepțiilor nu sunt un lucru nou, însă tehnologia care sprijină acest gen de război este foarte căutată în zilele noastre. Putem considera că prețurile, riscurile și utilizarea eficientă a războiului informațional pot fi foarte atrăgătoare. Avem nevoie de a arunca o privire mai adâncă asupra războiului percepțiilor pentru a-i înțelege importanța, ca tip de război.

Pepper (1967) vedea actele de percepție ca legături active conștiente între datele primite senzorial și mediul înconjurător. În formele sale cele mai simple, percepția necesită un obiect care să fie perceput și un observator. Când spunem „văd un scaun", scaunul este obiectul de referință și „eu" este cel care observă. Filosofic vorbind, poate exista o dispută privind existența unei referințe obiective, independente de datele senzoriale pe care le percepem.

---

[39] J. Glenn, J. Peterson, *Information Warfare, Cyber Warfare, Perception Warfare and their Prevention*, World Future Society, Atlanta, 1995.

Filosofii idealiști s-au confruntat cu datele, iar filozofii realiști cu independența celui care observă și referințele actului de percepție. În funcție de punctul de vedere pe care-l adoptăm, vom avea obiective diferite. Pepper, ca psiholog cognitiv susține o sinteză a perspectivelor idealiste și realiste și realizează acest lucru concentrându-se asupra observatorului ca participant activ în procesul de percepție, perspectivă care se concentrează asupra naturii percepției.

Pentru a clarifica ceea ce înțelegem prin războiul percepției mă voi referi la un exemplu teoretic de atac și apărare de percepție. Să presupunem că partea **A** are o sursă care îi asigură un avantaj asupra părții **B**. Dacă **B** e interesat să limiteze acest avantaj, poate distruge efectele sursei sau poate încerca să manipuleze percepția lui **A** în privința importanței sursei sale în legătură cu alte obiecte.

Un ultim efort poate fi realizat prin mai multe mijloace, dar având o baza comună: manipularea percepției lui **A** asupra sursei sale. Această manipulare poate fi realizată doar cunoscând procesul de percepție al celuilalt. Trebuie să fim atenți asupra modelelor care determină natura percepție lui.

Oamenii par să aibă capacități limitate de a percepe o situație [40]. Simon [41] a arătat că ceea ce diferențiază un novice de un maestru în șah este capacitatea de a vedea șabloanele în situațiile care evoluează după structuri cunoscute, dar dacă nu este nici o structură, maestrul nu are nici un avantaj. În mod similar, un atac asupra percepției este un atac asupra capacităților unui conducător de a găsi structuri potrivit viziunii sale asupra situației date.

Pierzându-și structura, conducătorul nu mai poate vedea șabloanele logicii. În schimb, un atac poate crea structuri care să formeze modele, care îi determină pe conducători să acționeze într-un anume fel. Problema este că oamenii sunt impredictibili și

[40] G. Miller :"The Magical Number Seven, Plus or Minus Two", *Psichological Review,* 1956.

[41] H. Simon, „Making Management Decisions: the Role of Intuition and Emotion", *Academy of Management Executive,* 1987.

e foarte dificil să prevezi rezultatul unui atac asupra percepției. Totuși, o privire în interiorul războiului percepțiilor ne dă o imagine asupra a ceea ce e important de protejat și a ceea ce poate fi manipulat.

Miezul problemei îl constituie aflarea modului în care comandantul își creează propria conștientizare a situației și ce pre-înțelegere putem presupune că are. Procesul conștientizării situației de către comandant și atitudinile sale vor fi obiectivele principale ale unui potențial atac și elementul principal de protejat. Sun Tzu afirma: „Cine înțelege cum să utilizeze atât forțele fizice cât și pe cele psihice, va fi victorios" (Griffith, 1971, p.82). Sun Tzu voia să spună că trebuie să vedem diferitele niveluri ale problemei care ne pot conduce spre succes. Sun Tzu conchide că un comandant aflat într-o stare de confuzie determină victoria celuilalt. Conceptia sa asupra confuziei poate fi înțeleasă ca pierderea controlului asupra situației.

Studii recente asupra războiului modern au arătat că abilitatea de a crea sisteme de conștientizare este factorul cheie pentru a controla și a avea succes în război. Putem descrie războiul modern că fiind lupta adevărurilor. Într-o luptă a încrederii căutăm nu doar adevărul, ci încercăm și să-l controlăm.

O întrebare filosofică tradițională este: ce e adevărul? Discuțiile sfârșesc de cele mai multe ori prin a concluziona că depinde de situație. Modul nostru de abordare a acestei probleme este că adevărul este o construcție socială, bazată pe înțelegeri și încredere.

Din această perspectivă, ce este adevărat pentru mine nu e în mod necesar adevărat pentru altcineva, dar de cele mai multe ori e vorba de o înțelegere asupra a ceea ce pare să fie imaginea generală a realității. Adevărul este atunci legat de un sistem de norme.

Conceptele tradiționale despre războiul informațional presupun că există un singur adevăr și că războiul înseamnă a avea capacitatea manipulatorie de a vedea adevărata imagine a

situației. Însă, doar cu un singur adevăr, războiul informațional va trebui să creeze informația privind maniera generală de a percepe realitatea, cu alte cuvinte, va crea ceea ce lumea crede că este adevărat. Influențarea sistemului de norme este un proces care ia mult timp, ceea ce nu corespunde înțelegerii comune a războiului informațional. Războiul informațional implică scopuri clare, care să fie realizate într-o perioadă de timp relativ scurtă [42].

Războiul este un fenomen haotic, caracterizat de o anumită incertitudine. Primul lucru pierdut în război este capacitatea de a crea o imagine a ceea ce pare a fi adevărat. Atât observatorul cât și sistemul de norme vor fi afectați de acest lucru. Rumoarea și dezinformarea vor face dificilă estimarea accesibilității informației și decidentul va fi nevoit să acționeze pe baza unor informații incomplete. În această situație, tot mai avem o opinie despre ce să credem și ce nu, fapt care se sprijină pe modul în care percepem situația.

Ceea ce pare să fie adevărat sau nu se va sprijini pe structurile individuale de credințe, care se pot modifica de-a lungul timpului. Încrederea este o construcție socială și poate fi extinsă și manipulată. Războiul percepțiilor nu înseamnă modificarea adevărului, ci crearea lui. În ambele cazuri, adevărul este o victimă.

Pentru a înțelege cum poate fi influențată imaginea unui comandant asupra unei anumite situații trebuie să înțelegem ce face comandantul. Într-o descriere abstractă ar trebui să vedem comandantul ca un sistem cibernetic în care acesta acționează prin intermediul deciziilor, care se sprijină pe imaginea pe care o are despre situația dată. Rezultatul acțiunilor ne dă noi elemente de feed-back. Acestea schimbă imaginea asupra situației, care necesită în schimb noi acte [43].

Imaginea conandantului asupra situației poate fi descrisă în termeni de conștientizare situațională, bazată pe propriile-i

[42] A. Codevilla, *Informing Statecraft*, 1992.

[43] J. de Rosnay, The Macroscope, Harper & Row, Publishers, New York, 1979.

observații și pre-înțelegeri. Preînțelegerile sunt proprii fiecărui comandant și depind de context, ceea ce explică de ce aceleași informații pot conduce la acțiuni diferite. Această conștientizare situațională se sprijină pe factori raționali și emoționali. Elementele imaginii sunt logice, din punct de vedere rațional și al structurilor, dar unele par să fie iraționale, având la bază emoții. Putem descrie părțile logice în modele și deci face predicții, dar în privința părții emoționale avem doar sentimente intuitive.

Vulnerabilitatea reală a comandantului o constituie chiar mintea sa și maniera în care înțelege o situație dată. „Înrobește-i mintea, inima și sufletul și vor putea fi distruși". Imaginea pe care o creează mintea comandantului nu e în mod necesar adevărată, dar ea îi ghidează acțiunile.

Comandantul va continua să aprecieze cât de mult crede că are controlul asupra situației, în termeni de incertitudine și riscuri. Controlul este construit prin explicații logice ale situației, având informațiile structurate potrivit diferitelor șabloane. Cautând mai multă informație, va încerca să limiteze incertitudinea.

În această perspectivă, războiul percepțiilor reprezintă capacitatea de a influența imaginea comandantului asupra unei anumite situații, într-un mod bine controlat, arta de a influența deciziile. Este important ca această influențare să fie un proces controlat. Altfel, există riscul luării unor decizii nefavorabile.

E important de reamintit că nici un comandant nu dorește să fie văzut ca un învins. Într-un atac al percepțiilor reușit, fiecare participant trebuie să creadă că el e învingătorul. De aceea, scopul unui astfel de atac este de a crea iluzia (percepția) că fiecare este un învingător.

Nu e un joc cu suma nulă, în care succesul unei părți înseamnă insuccesul celeilalte părți. În realitate, unii câștigă mai mult decât alții. Percepția situației este elementul cheie al modului în care va acționa comandantul.

Mintea este centrul de gravitație al unui atac. Capacitatea unui comandant de a crea o imagine satisfăcătoare a situației este

determinantă pentru activitățile viitoare. Adevăratul inamic în războiul percepțiilor este mintea comandantului și nu, în primul rând, adversarul. Adversarul va încerca în orice mod să creeze o imagine conformă scopurilor sale și cea care creează actuala imagine a situației este mintea comandantului.

Întrebarea este atunci cum să ne apărăm mintea, lucru care în multe privințe seamănă cu problema virușilor de computer, dar care necesită găsirea altor soluții. În lumea calculatoarelor, cea mai bună măsură de securitate este aceea de a deconecta calculatoarele de la rețele, utilizând doar calculatoare individuale cu coduri de acces. Această metoda nu e de dorit a fi folosită în cazul indivizilor care au nevoie de interacțiune socială. Trebuie găsite noi căi pentru verificare și autorizare care să ne ajute să descoperim atacurile de percepție.

O minte deschisă este necesară pentru a rezolva problemele în mod creativ, dar, o minte deschisă este, în același timp, și vulnerabilă la interferențe străine. Războiul percepțiilor este o luptă dusă la un nivel individual, în care comandantul este „ținta". Scopul este de a introduce un sentiment de nesiguranță în privința problemelor pe care comandantul le consideră importante.

Nesiguranța este concepută în termeni de pierdere a controlului. Dacă pierdem controlul, pierdem și perspectiva a ceea ce facem pe termen lung și riscăm să trecem de la condiția de lider la cea de masă, care urmează un lider. Acest lucru creează oportunități pentru adversar în a ne condiționa comportamentul și deciziile viitoare. De obicei, liderul e mai ușor de identificat ca obiect, decât masa.

Pentru a putea prelua controlul, trebuie să știm ce consideră important comandantul (ca „observator") și cum putem exploata acest lucru. De exemplu, dacă acesta apreciază că a fi punctual este un lucru important, îi putem induce o stare de stres întârziind informația. Dar nu e suficient. Cât de veche poate fi considerată informația și cât de mult poate fi considerată ca fiind de ultimă oră? Problema percepției este o problemă de atitudine, care stă la baza modului în care apreciem situația.

Scopul final al unui război de percepție e de a schimba modul de gândire și modul de manifestare a voinței. Spre deosebire de războiul tradițional, toate părțile implicate într-un război al percepțiilor pot avea impresia că sunt învingători.

CONCLUZII

În acest material am încercat să clarificăm conceptul de război al percepțiilor. Scopul principal a fost definirea problemelor și direcțiilor pentru o viitoare cercetare asupra acestui subiect, mai degrabă decât discutarea în detaliu a oricărei din aceste probleme. Un astfel de demers va fi făcut într-un viitor material. Totuși, chiar și din această discuție introductivă ar trebui să fie clar că există multe lucruri pe care nu le știm și că este nevoie de multe cercetări înainte de a realiza un concept al războiului percepțiilor. Pentru a conceptualiza ceea ce este schițat deja, trebuie să ne concentrăm asupra unor serii de pași și a unor studii în această direcție.

OPERAȚIILE INFORMAȚIONALE PERSPECTIVA NATO

General maior JOSE GARDETA

Evoluția globală a tehnologiei a schimbat lumea. Informația nu numai că integrează acum cele mai multe elemente ale vieții moderne, incluzând comunitatea civilă și militară, dar și accelerează toate procesele.

Această schimbare a condus la necesitatea ca NATO să examineze îndeaproape toate sistemele implicate, având mereu în vedere posibilul impact al informației. Acest lucru a condus la dezvoltarea politicii NATO pentru operații informaționale conținută în documentul Comitetului Militar MC-422, care a fost aprobat de Consiliul Nord Atlantic.

Operațiile informaționale sunt acțiuni întreprinse pentru a influența factorii de decizie în conformitate cu anumite obiective politice și militare, prin afectarea informației ca și prin afectarea proceselor care se bazează pe informație. Operațiile informaționale integrează războiul de comandă și control cu procesul de consultare politică, aparatul de luare a deciziei și cu operațiile politico-militare ale Alianței. Îi asigură comandantului o modalitate de implementare a acestui nou tip de abordare, în procesele de planificare.

În mod similar, asigură și o concentrare a eforturilor pe apărare. Schimbarea operațională importantă constă în concentrarea pe rolul informației. Acest lucru include aspectele semantice sau de percepție, ca și pe cele tehnice (fizice și logice). Planificarea militară nu necesită numai implicare directă a aparatului politic de luare a deciziei, dar și o implicare și o integrare largă a unor elemente din conducere.

Subiectul „operații informaționale" devine tot mai critic pe zi ce trece, pentru națiuni. Operațiile informaționale au capacitatea de a atinge inima unei națiuni, să aducă prejudicii infrastructurii, să aducă atingere acelor lucruri care-i permit unei națiuni să existe.

Unul dintre cele mai mari câștiguri, ce poate fi exploatat de pe urma folosirii operațiilor informaționale, este abilitatea lor de a preveni dezvoltarea unei crize în conflict prin mijloace și metode care demonstrează potențialului adversar că escaladarea respectivei crize nu este în interesul său. În acest sens, activitățile trebuie să fie conduse pe timp de pace și ar trebui să fie sprijinite atât politic cât și militar, să cunoască atât punctele tari cât și cele slabe și să se concentreze pe acele zone care sunt cele mai eficiente în atingerea obiectivului final.

Probabil că cel mai îngrijorător aspect în dezvoltarea operațiilor informaționale este faptul că nu există o înțelegere generală a ceea ce sunt acestea cu adevărat. Cei mai mulți sunt familiarizați cu diferite părticelepe care le consideră din păcate că reprezentând întregul. Olanda recunoaște importanța operațiilor informaționale ca și importanța implicațiilor lor. Un indice important al acestei înțelegeri este studiul bilateral întreprins de Olanda și de Germania.

Operațiile informaționale nu sunt un concept nou, ele sunt rezultatul evoluției eforturilor noastre în dezvoltarea sistematică a abordării războiului. Manifestări mai moderne ale evoluției se găsesc expuse de către Von Clausewitz în cartea sa, „Despre război", unde autorul discută principiile războiului.

Mai recent este însă conceptul Statelor Unite, Joint Vision 2010, în care este abordată o nouă modalitate de implementare a cerințelor operațiilor informaționale. Aceste aspecte, precum și alte numeroase încercări de organizare eficientă a armatelor, plus tehnologia informațională, ne-au condus astăzi la adoptarea prezentei poziții.

Înainte de a ne concentra analiza asupra operațiilor informaționale, voi aminti strategia care a condus la dezvoltarea operațiilor informaționale, o strategie care a fost executată aproape perfect de către aliați în războiul din Golf. Această strategie este comanda și controlul.

Războiul de comandă-control este definit în MC-348, „Politica războiului de comandă-control", astfel: *„Folosirea integrată a tuturor capacităților militare, inclusiv operațiile de securitate (OPSEC), inducere în eroare, operații psihologice (PSYOPS), război electronic (EW) și distrugere fizică sprijinită de către toate sursele de intelligence și CIS, pentru interzicerea accesului la informație, influențarea, degradarea sau distrugerea capacității* C2 *a unui adversar în timp ce sunt protejate toate acestea împotriva unor acțiuni similare".*

Cu alte cuvinte, războiul de comandă-control înseamnă exact ceea ce afirmă și denumirea sa, executarea de acțiuni pentru prevenirea controlului adversarului asupra informației necesare pentru realizarea de evaluări și decizii corecte privind controlul și folosirea bunurilor sale.

Figura 1 ilustrează cum cei cinci piloni ai războiului de comandă-control sunt discipline individuale, iar atunci când există coordonare și sprijin ferm din partea intelligence-ului și comunicațiilor, întregul pe care ei îl produc, războiul de comandă-control, este mult mai mare decât suma tuturor părților.

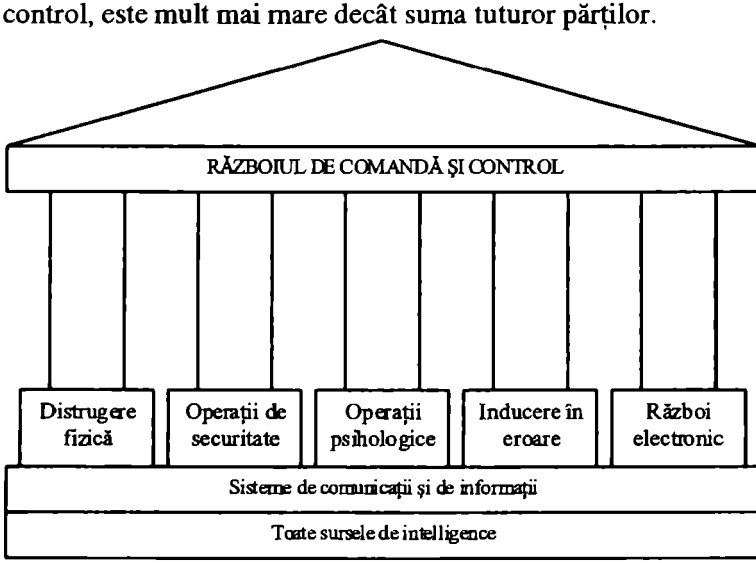


Figura 1: Cei cinci piloni ai războiului de comandă-control

Războiul de comandă-control se referă la coordonare. Prin folosirea celor cinci piloni și a altor capacități militare într-o manieră coordonată, se obține o sinergie care permite operarea extrem de eficientă în cadrul unei crize/conflict. Operațiile informaționale nu înlocuiesc războiul de comandă-control, dar integrează această strategie militară în procesul de consultare politică, în aparatul de luare a deciziei și le combină cu operațiile politice și militare ale Alianței.

Cu alte cuvinte, **războiul de comandă-control este aplicarea militară a operațiilor informaționale**. NATO are o experiență considerabilă cu războiul de comandă și control și-l execută ireproșabil. Alianța a aprobat politica în MC-348 încă din 1995, și de atunci fiecare OPLAN a conținut o anexă de război de comandă și control.

În timp ce războiul din Golf este în general recunoscut ca primul război informațional, nu atunci s-a folosit pentru prima dată războiul de comandă-control în luptă. De-a lungul secolelor, comandanții au știut că impiedicarea adversarului de obținere a informației este un excelent mijloc de sabotare a campaniei sale.

Cum se poate în acest amestec de informație ca pe de-o parte să prevenim ca informația critică să ajungă la inamic, în timp ce pe de altă parte să prevenim efectul opus? O bună parte din răspuns rezidă în planificarea la toate nivelele operaționale și tactice. Dar azi, în actualul mediu internațional, planificarea nu trebuie să fie strict delegată sectorului militar, și această afirmație se referă îndeosebi la NATO,atunci când se are în vedere faptul că toate capacitățile militare ale NATO derivă din cele 19 națiuni, efectele pe care operațiile informaționale le pot avea asupra NATO devin clare.

Operațiile informaționale sunt interesate de obiective informaționale, pe care un comandant caută să le atingă prin acțiunile sale. Operațiile informaționale au impacturi diferite la diverse nivele de război, din moment ce fiecare nivel este diferit. La nivel strategic, operațiile informaționale sunt folosite în

sprijinul obiectivelor NATO. Acest sprijin este obținut prin influențarea sau afectarea tuturor elementelor (politice, militare, economice sau informaționale) a puterii naționale a adversarului, în timp ce sunt protejate cele ale NATO.

La nivel operațional, operațiile informaționale se concentrează pe sprijinul obiectivelor operaționale majore. Impactul major la acest nivel este simțit de către liniile de comunicare, logistică și comandă-control ale adversarului. La nivel tactic sprijină îndeplinirea obiectivelor tactice specifice.

O definiție a operațiilor informaționale, așa cum reiese din MC-422, care este intitulată „Politica NATO a operațiilor informaționale", aprobată de către Comitetul militar pe 15 decembrie 1998 și de către Consiliu pe 22 ianuarie 1999: operațiile informaționale sunt definite ca *„acțiuni întreprinse pentru a influența factorii de decizie care sprijină anumite obiective politice și militare, prin afectarea informației altora, a proceselor care se bazează pe informație, a sistemelor* C2 *și CIS în timp ce exploatează și protejează propria informație și propriile sisteme informaționale."* Există două categorii principale de operații informaționale: operațiile informaționale defensive și operațiile informaționale ofensive.

Unele dintre capacitățile folosite în cadrul operațiilor informaționale defensive includ: asigurarea informației, operațiile de securitate (OPSEC), securitate fizică, contra-inducere în eroare, contra-propaganda, contra-intelligence și război electronic. Operațiile informaționale ofensive pot de asemenea să sprijine operațiile informaționale defensive. Sistemele informaționale servesc drept înlesnitori, care întăresc capacitățile de luptă; faptul că NATO se bazează tot mai mult pe aceste sisteme creează vulnerabilități.

Este imposibil să protejezi complet toate sistemele, tot timpul. De aceea trebuie protejate bunurile relative la valoarea informației pe care le conțin și riscurile asociate cu pierderea sau degradarea acelei informații. Această valoare va varia bineînțeles în timp.

Există mai multe procese implicate care interrelaționează cu operațiile informaționale defensive, și care includ protecția mediului informațional: capacitatea de a detecta atacuri asupra sistemelor; capacitatea de a restaura sistemele pentru a putea folosi acest tip de atac și de a avea capacitatea de a răspunde unui astfel de atac.

Operațiile informaționale ofensive implică folosirea integrată a capacităților și activităților desemnate, sprijinite de intelligence, cu scopul de a afecta factorii de decizie adverși și de a obține și promova obiective specifice. Capacitățile folosite în acest scop includ, dar nu sunt limitate numai la, operații de securitate (OPSEC), inducere în eroare, operații psihologice (PSYOPS), război electronic (EW), atac fizic/distrugere și atac asupra rețelei de computere.

După părerea mea, NATO va acționa, în special în situații de răspuns la criză și datorită naturii alianței care are nevoie de consensul celor 19 națiuni suverane pentru a proba și implementa acțiunile. Sistemele naționale juridice complică și mai mult această problemă, din moment ce, în unele cazuri, unele activități sunt considerate a fi ilegale.

Cred că înseamnă folosirea tuturor capacităților care sunt la îndemână pentru protecția propriei informații, a sistemelor și proceselor care se bazează pe informații, în timp ce se încearcă atingerea celor ale adversarului. Atunci când sunt analizate capacitățile, cel mai potrivit punct de plecare este războiul de comandă și control: războiul electronic, operațiile de securitate (OPSEC), inducerea în eroare, distrugerea fizică și operațiile psihologice (PSYOPS). A nu se confunda: operațiile informaționale înseamnă mai mult decât cele cinci elemente ale războiului de comandă și control.

Lanțul de comandă se extinde mult și la nivelul adversarului și la conducerea sa civilă. În mod cert, ramificările folosirii majorității capacităților războiul de comandă și control împotriva unei națiuni constituie un act de război. Dar tot atât de clar este și

faptul că dacă, conducerea părții adverse de la acel nivel poate fi afectată, un conflict iminent poate fi evitat. Dar, pe timp de pace, conducerea politică nu este o țintă militară legitimă. Astfel se poate vedea dilema cu care se confruntă planificatorii militari pe măsură ce ei continuă să dezvolte procesul C2W.

Operațiile psihologice au un loc special în cadrul războiului de comandă și control și al operațiilor informaționale, din mai multe motive. Printre altele, furnizează militarilor mijloacele de influențare a conducerii adversarului, a trupelor sau chiar a populației, pe timp de pace.

În ciuda acestei capacități, pe care eu o consider ca o punte între războiul de comandă și control și operațiile informaționale, operațiile psihologice sunt așa de maligne încât doar simpla lor menționare în anumite cercuri conduce la reacții nefavorabile. Acest lucru este valabil, mai ales în mediul politic. Membrii acestor instituții înțeleg trei puncte importante despre relația dintre operațiile psihologice și aducerea la cunoștință pentru publicul larg, a diferitelor informații.

În primul rând, operațiile psihologice sunt acuzate de planificarea și executarea proiecției de activități care intenționează să informeze persuasiv grupurile țintă și populația. Intenția operațiilor psihologice nu este propaganda sau minciuna ca furnizarea informațiilor adevărate sau a declarațiilor atunci când interesele noastre sunt cel mai bine servite. De fapt și de drept, minciuna este contra productivă pentru că o dată descoperită toată credibilitatea este pierdută.

Atunci când sunt folosite așa cum trebuie, tehnicile operațiilor psihologice pot scădea moralul și reduce eficiența forțelor dușmane și pot crea dizidență. În al doilea rând, operațiile psihologice și informarea publicului larg trebuie să se coordoneze. Operațiile psihologice au un impact major asupra fluxului de informație. Momentul în care se produce informarea publicului poate fi modificat astfel încat să vină în sprijinul percepțiilor stabilite de către operațiile psihologice.

În cele din urmă, operațiile psihologice executate pe timp de pace vor avea o altă concentrare decât atunci când sunt folosite pe timp de criză sau conflict. Eforturile pe timp de pace se concentrează pe operațiile militare altele decât războiul, precum Operațiile de Sprijin al păcii (PSO), asistența umanitară și sprijin în caz de catastrofă naturală. Pe timpul conflictului, operațiile psihologice sunt folosite ca orice altă capacitate de sprijin a realizărilor obiectivelor comandantului.

Partea politică a Alianței ar trebui să vadă operațiile psihologice ca partener al activităților de informare publică, și nu ca un competitor, și în mod cert nu ca o mașină de propagandă. Operațiile psihologice sunt o capacitate pur militară și de aceea nu pot să fie înlocuite sau subordonate informării publice. Așa cum am afirmat și mai devreme, planificarea și coordonarea folosirii operațiilor psihologice și informării publice au potențialul de a preveni izbucnirea ostilităților.

Digresiunea noastră asupra operațiilor psihologice nu a fost în zadar. A adus în mod subtil în discuție un alt fapt care, în opinia mea, este cel mai important aspect al operațiilor informaționale.

Acum că am văzut de unde a provenit conceptul NATO de operații informaționale și cum l-am definit, aș dori să vă răpesc, puțin din timpul dumneavoastră, pentru a analiza cum se pot implementa operațiile informaționale. Cred, de asemenea, că este absolut necesar să subliniez câteva schimbări fundamentale care au avut loc în ultimii zece ani, și care au influențat în mod semnificativ modul în care armatele NATO fac față crizei sau conflictului.

Evoluția globală a tehnologiei în domeniul informației a schimbat lumea. Informația nu numai că a integrat cele mai multe elemente ale vieții moderne, dar a și accelerat toate procesele. Viteza cu care putem să transmitem informația, volumul de informație sunt fără precedent. Azi avem posibilitatea a trimite o cantitate aproape nelimitată de informație, în numai câteva secunde. Miniaturizarea computerului a făcut din el un echipament standard, chiar și pe câmpul de luptă.

Tehnologia este doar unul dintre regimurile operațiilor informaționale. Un alt aspect pe care l-am atins puțin atunci când am discutat despre operațiile psihologice. Acesta este regimul semantic sau cognitiv. Partea tehnică este probabil mai bine înțeleasă probabil decât cea semantică deoarece implică lucruri cu care suntem obișnuiti, echipament și folosirea sa.

În timp ce operațiile informaționale se concentrează pe soluții non-kinetice, trebuie să avem mereu în vedere că distrugerea fizică, unul dintre cei cinci piloni ai războiului de comandă și control, este de asemenea un element al operațiilor informaționale. Partea cognitivă include capacitățile găsite în informarea publică, operațiile psihologice și operațiile mass-media.

Războiul rece a furnizat Alianței „o situație de planificare ideală": perioade lungi de tensiune, zone cunoscute de angajare, adversari cunoscuți și înțeleși. Principala funcție a aparatului politic în ce privește conflictul era să decidă dacă NATO trebuia sau nu să se implice, și dacă da, să declare implicarea sa. Exista puțină implicare politică o dată ce conflictul era declarat și se desfășura.

Azi, circumstanțele diferă considerabil. Așa cum s-a demonstrat și prin operațiile forței aliate, NATO este azi constrâns de implicarea politică în timpul unei crize. Acest lucru înseamnă că autoritățile politice controlează sectorul militar. Militarii trebuie să se miște în mediul creat de politicieni.

Un bun exemplu al acestei situații rezultă și din declarația Alianței că nu va folosi trupe terestre pentru conflictul din Kosovo. În mod cert, această decizie a fost o manevră politică din partea NATO. Impactul acțiunilor militare asupra sensibilităților, implicațiilor și imperativelor politice în conducerea operațiilor trebuie să fie pe deplin înțelese atât de structura militară cât și de cea politică.

O altă variabilă care trebuie luată în considerare este sensitivitatea națională. Sensibilitățile naționale au fost o grijă majoră a NATO, și așa și trebuie să fie într-o alianță în care

deciziile se bazează pe consens. Cu toate acestea, în zilele războiului rece, aceste sensibilități nu aveau un impact prea puternic asupra stipulărilor articolului V și asupra alocărilor de resurse naționale pentru NATO, așa cum se întâmplă azi în era informațională.

Așa cum am menționat mai înainte, multe dintre resursele noastre au fost croite pentru a veni în întâmpinarea cerințelor tipurilor de scenarii din articolul V, pe care NATO le planifică de ani de zile.

Două exemple a celor mai importante resurse la care fac referire sunt capacitățile operațiilor ofensive și intelligence. Aceste capacități sunt foarte atent păzite de către națiuni, ceea ce înseamnă că acestea vor ezita în a aloca resurse Alianței.

Un alt factor important, pe lângă sensibilitățile naționale și legătura lor cu alocarea de resurse este opinia publică. Azi scene de luptă intră în casele noastre aproape fără întârziere; războiul așa cum este văzut de CNN este o regulă. În mod evident, opinia publică este extrem de importantă pentru politicieni și va afecta cu siguranță deciziile lor în ce privește resursele.

O altă și ultimă schimbare, pe care o vom lua în discuție, și care pentru noi militarii este mai ușor de înțeles deoarece ne confruntăm cu ea în fiecare zi, este intelligence-ul. Planificarea, executarea și evaluarea activităților de operații informaționale este imposibilă fără un sprijin adecvat din partea intelligence-ului. Acest lucru pune însă Alianței o serioasă problemă, deoarece ea nu posedă capacitatea organică de a aduna și procesa datele cerute pentru dezvoltarea intelligence-ului.

În plus, nu există un aparat politic/militar de intelligence în funcțiune în cadrul NATO. Și pe deasupra, cerințele de intelligence pentru operațiile informaționale sunt diferite față de cele care se găsesc în mod tradițional în armată.

Intelligence-ul trebuie să fie la timp, precis, ușor de folosit, complet, relevant, la obiect și suficient de detaliat pentru a sprijini cerințele NATO. Operațiile informaționale au nevoie de răspuns

la o întrebare pe care comunitatea de operații nu a mai pus-o niciodată intelligence-ului: de ce? În trecut erau necesare „doar faptele". În lumea operațiilor informaționale, acest gen de informație nu mai este suficientă pentru a face o treabă bună.

Intelligence-ul contribuie de asemenea și la procesul de detectare a atacului prin furnizarea de avertismente, prin evaluarea activității potențiale a adversarului și prin culegerea de indici specifici de activitate.

În plus la toate acestea, comunitatea operațională trebuie să fie foarte precisă în descrierea cerințelor comunității de intelligence. Un prim pas în dezvoltarea cerințelor de intelligence constă în determinarea de unde vor veni amenințările pentru NATO. Apoi este necesară determinarea dacă acea națiune sau acel grup anume posedă capacitatea de a întreprinde operații informaționale.

Pe scurt, datele problemei pentru NATO s-au schimbat în mod dramatic, față de acum 10 ani. Lumea militară nu trebuie doar să accepte acest lucru, ci să se și adapteze la aceste schimbări.

În mod cert, situația descrisă mai sus are un impact de proporții asupra operațiilor militare, incluzând și operațiile informaționale. Acest lucru este adevărat mai ales la nivel strategic politic/militar. Așa cum am menționat și mai înainte operațiile informaționale ale NATO nu trebuie considerate ca fiind o nouă strategie. Dar viteza și volumul cu care transmitem informația, precum și aria de aplicabilitate au schimbat complet impactul general al informației asupra interfeței politice/militare.

Ce înseamnă toate aceste lucruri pentru NATO și cum poate Alianța să profite de oportunitățile oferite de operațiile informaționale? În mod cert, primul pas este elaborarea unui plan. Pentru acest plan este important să păstrăm în minte toate condițiile noi.

În primul rând trebuie să ne antrenăm liderii și personalul cu roluri cheie pentru a fi în măsură să gândească diferit.

Trebuie să înțelegem că documentația nu ne va furniza întotdeauna certitudinile cu care suntem obișnuiți sau pe care le

căutăm. Prezenta situație și orientarea politică vor dicta cum vor acționa și reacționa militarii într-un conflict.

Una dintre cele mai importante lecții care ne-au fost date de Kosovo, constă în faptul că armatele se mișcă într-un mediu creat de politicieni. La rândul lor, politicienii trebuie să înțeleagă consecințele militare ale deciziilor pe care le iau.

Să ne întoarcem acum la planul pentru operațiile informaționale ale NATO. Structura nivelului de lucru de fiecare zi este în funcție. Trebuie acum să dezvoltăm mecanismul de ghidare și direcționare a programelor pentru a obține un beneficiu maxim pentru Alianță. În acest scop, am stabilit:

Grupul de lucru NATO pentru operații informaționale. Acest comitet este prezidat de un Flag Officer, și are membrii permanenți: națiunile, comenzile strategice (SC Strategic Comands), un președinte pe probleme juridice pentru zonele funcționale, care cuprind elemente de război de comandă-control, de exemplu operațiile informaționale, conducerea internațională/ treburi politice și Subcomitetul NATO de securitate informațională (INFOSEC).

Pe timpul participării noastre la campania de operații informaționale din Kosovo, a devenit limpede că nu există o înțelegere comună a operațiilor informaționale sau a cerințelor pentru stabilirea unei campanii. Dezvoltarea avertizării timpurii este extrem de importantă în acest context.

Noi am mai realizat ceva și în partea defensivă, cea care este administrată de către NHQC3S.

Conducerea C3 a NATO a început să studieze multe aspecte ale operațiilor informaționale. Ea a însărcinat Subcomitetul INFOSEC să dezvolte viziunea NATO de asigurare a informației. Discuțiile în această zonă s-au concentrat pe rolurile Comitetului Militar și ale NC3B via INFOSEC SC. Un document care tratează problemele ridicate de asigurarea cu informații este acum în cea de-a doua sa revizie. Pe lângă aprobarea SC, acest document va fi înaintat spre aprobare lui NC3B.

În plus, NC3B a însărcinat Subcomitetul INFOSEC cu dezvoltarea implementării planului pentru CERT (Computer Emergence Response Team). Această echipă va asigura utilizatorilor CIS avertizări prompte la adresa securității lor și sfaturi. Realizarea unei astfel de echipe va avea impact atât asupra mediului militar, cât și civil a organizării NATO.

Din nou trebuie amintit că dezvoltarea avertizării de timpuriu este extrem de importantă. Mijloacele primare prin care urmărim dezvoltarea acestei capacități sunt cursurile la școala NATO, SHAPE, participarea la forumurile naționale, la seminariile profesionale și la grupurile, organismele și agențiile NATO. Participarea noastră la Simpozionul din Academia Militară Regală a Olandei, din 3 decembrie 1999, este un exemplu.

Operațiile informaționale trebuie să devină o parte integrantă a procesului de planificare operațională. Operațiile informaționale sunt aplicabile în orice fel de condiții, de la pace la criză și război și înapoi la pace. Lor le este furnizată orientare politică clară din partea Consiliului, și vor juca un rol cheie atunci când sunt implementate toate aspectele conceptului.

Mai trebuie să ating și aspectul dependenței evidente a NATO de capacitățile națiunilor, de exemplu intelligence, capacități care sunt vitale pentru planificarea și conducerea de operații informaționale.

Unele dintre capacitățile operațiilor informaționale ofensive dezvoltate de către națiunile membre ale Alianței sunt foarte sensibile și destul de scumpe, și de aceea nu vor fi asigurate de către națiuni. De aceea este prudent din partea NATO să-și dezvolte niște capacități organice ofensive.

Operațiile informaționale pe timp de pace, dacă sunt descoperite de către țintă pot foarte bine să fie considerate provocatoare, ba chiar ostile, și pot de aceea să necesite autorizare politică clară din partea Consiliului.

Două din cele mai importante componente ale operațiilor informaționale, intelligence-ul și comunitățile de CIS, vor fi foarte

mult implicate în determinarea și abordarea amenințărilor sistemelor noastre și a vulnerabilităților sistemelor noastre la aceste amenințări. Ca un minim necesar, este de dorit ca noi să determinăm sistemele critice care trebuie protejate pentru a putea proteja funcționarea pe mai departe a NATO.

Cu scopul de a verifica și pune în practică aceste proceduri este necesar să includem operațiile informaționale în cadrul exercițiilor NATO.

Dezvoltarea unei doctrine de operații informaționale trebuie să fie inițiată cât de curând. Doctrina este un compendiu de lecții învățate. Operațiile în Balcani vor furniza cu siguranță un material excelent pentru acest document. Să ne amintim mereu că operațiile informaționale sunt un mod de gândire și nu neapărat ceva ușor de cuantificat.

CONCLUZIE. În concluzie, permiteți-mi să mai subliniez încă o dată că operațiile informaționale nu sunt ceva nou. Ceea ce este nou este procesul de gândire, pe care-l mandatează operațiile informaționale.

A INFORMA, CHIAR ÎN CONDIȚII DIFICILE..

Col. EDWIN HOFSTETTER
Elveția

Într-un stat democratic, cum este și Elvetia, cenzura mass-media este ceva de neconceput. Guvernul elvețian a decis să creeze un „regiment informațional" care să acționeze dacă, în anumite circumstanțe, activitatea normală a presei, radioului și televiziunii este pusă în pericol. Acest articol descrie istoria, misiunile și organizarea acestui regiment.

În anii de dinaintea celui de al doilea război mondial, circumstanțe politice dificile influențau eforturile de informare a populației și forțelor armate. Instituțiile germane erau în plină desfășurare a unei bătălii de propagandă la o scară mare, chiar și împotriva Elveției.

Majoritatea presei elvețiene reușea să combată această propagandă, reflectând libertatea și autonomia țării. Guvernul și armata au încercat, prin îndrumare și control, să prevină apariția unor provocări la adresa Germaniei. La izbucnirea războiului, acest lucru a condus la cenzurarea presei.

O dispoziție a armatei în toamna lui 1939 a creat secțiunea „Heer und Haus" (Armata și Casa). Această organizație avea misiunea de a informa populația despre chestiuni legate de apărarea națională, cu scopul de a întări rezistența națională și de a menține identitatea națională. O rețea cu mai mult de 100000 de membri și 7000 de corespondenți din întreaga țară activa pentru informarea, în diferite limbi, a populației elvețiene, reușind în acest mod să ia și pulsul societății.

O altă structură, „Action National Resistance" - Rezistența

națională pentru acțiune, de această dată privată și neafiliată politic, completa acțiunile „Heer und Haus". Acțiunile acestor structuri erau coordonate de serviciul de intelligence și biroul de presă și radio al guvernului. La puțin timp după terminarea celui de al doilea război mondial o nouă organizație privată a luat ființă: Swiss Information Service (Schweizerische Auflarungsdienst - SAD).

În anii de dinaintea celui de al doilea război mondial, statul major elvețian a luat o serie de măsuri de prevedere, cum ar fi controlul presei. Când războiul a început, în 1939, armata a stabilit că ar trebui să existe o cenzură preliminară. Guvernul elvețian, Bundesrat, a anulat această măsură și a decis că cenzura va funcționa doar după publicare.

Discuțiile cu reprezentanții mass-media au dus la apariția unor reglementări, în concordanță cu legile constituționale și starea de război. La început, armata era responsabilă pentru cenzură și aplicarea acestor reglementări. Prin aceasta, departamentul presă și radio (Abteilung fur Presse und Rundfunk -APF) din statul major avea scopul de a proteja securitatea internă și externă a țării și neutralitatea sa, era responsabil de monitorizarea publicațiilor și transmiterea mesajelor și opiniilor prin telegraf, telefon, presă, radio, filme și imagini. Șeful statului major, gen. Guisan, nu considera însă cenzura presei ca o misiune a armatei ci, mai degrabă, ca o treabă politică.

Ca o consecință, în 1942 APF a fost subordonat directorului departamentului elvețian pentru justiție și poliție. Organizarea militară a APF a fost menținută și nu a fost modificat modul de realizare al cenzurei. Rapoartele și comentariile de politică externă au fost în special urmărite.

Editorii erau avertizați și unele ediții ale ziarelor erau oprite. Bundesrat-ul putea interzice publicarea unui ziar dacă considera că urmările acestei publicări ar impune. Aceste măsuri extreme au fost aplicate de aproape 60 de ori în cel de-al doilea război mondial.

Într-un stat democratic, cum este Elveția, cenzurarea mass-mediei este astăzi ceva de neconceput. Lecțiile învățate în timpul

războiului și noile tipuri de amenințări ale războiului rece au materializat ceea ce se numește „apărarea totală". Acest concept include, de asemenea, și comunicațiile, acestea trebuind să rămână sigure în caz de război, acțiuni teroriste sau catastrofe. APF a primit o nouă misiune, aceea de a funcționa ca mediu informațional între Bundesrat și populație.

Această nouă și complexă misiune a dus la suplimentarea personalului cu aproape 2500 de oameni. În 1982 a apărut o primă situație serioasă, în urma ocupării ambasadei poloneze de la Berna. În această situație Bundesrat s-a focalizat pe obținerea de informații din „surse deschise", acest lucru realizându-l APF.

Ofițerii APF au sprijinit, de asemenea, între octombrie 1998 și mai 1999, eforturile ministerului pentru refugiați. În același timp, misiunea principală a APF, aceea de a controla publicarea și comunicațiile, a fost menținută și pe timp de pace. Starea de pregătire a corpului 4 armată, componentă a gărzii de frontieră (Grenzwachtkorps) și a forțelor aeriene a fost testată în 1986. Acest lucru a fost realizat în cadrul unui exercițiu, de „apărare totală" în combinație cu manevre pe scară largă. Civili, organizații civile pentru starea de urgență și elemente ale transportului public au luat parte la acest exercițiu.

Aproape 250.000 de persoane din armată și civili au fost activ implicați timp de două săptămâni. APF a trebuit, cu o mie de oameni, să asigure, prin orice mijloace, funcțiunile informaționale ale exercițiului. Ca scenariu a fost utilizată o stare teoretică de criză. Toți participanții, ca și populația, au fost confruntați cu o situație imaginară de pericol: sirenele sună și la radio se anunța că există un pericol de radiație în urma unui „dezastru enorm în Franța, nu departe de Basel". Populația s-a adăpostit în adăposturi.

Mass-media a încetat, treptat, să funcționeze. Chiar și emisiile din străinătate erau foarte slabe. Telefoanele nu mai funcționau. În final, după aproape câteva ore, o voce se aude la radio: „Atenție! Aceasta este o transmisiune a APF, Departamentul pentru presă și radio. APF este instrunentul pentru informare al Bundesrat. Aveți încredere în vocea noastră..."

Transmisiile APF erau foarte puternice și pătrundeau și prin betonul adăposturilor. Prin aceasta, dar și prin alte mijloace, APF a dovedit că poate informa populația chiar și în condiții foarte dificile. Operațiunea „INFOSUISSE" a inclus folosirea radioului, televiziunii și presei. Transmisiunile TV ale APF prezentau de trei ori pe zi programe de 30 de minute în cele trei limbi vorbite în Elveția.

Pentru aproape cinci zile radiourile APF au transmis pe FM programe toată ziua, acestea incluzând știri, anunțuri speciale și muzică pentru populație și soldați. Prezentatorii, femei și bărbați, erau în general cunoscuți de la televiziunile și radiourile „normale". Ei erau rezerviști și au fost activați ca membri ai APF. Scopul principal era să se creeze o stare de încredere a populației în persoanele care o informează.

Ținta finală a acestui exercițiu, destul de greu de atins pe timp de pace, a fost de a întruni cerințele psihologice ale actului de informare a populației. Într-o situație reală periculoasă, APF ar trebui să mărească solidaritatea și dorința fiecăruia de a supraviețui, să reducă incertitudinea și să mărească încrederea în organele de conducere ale țării.

Publicul larg a acceptat radioul și televiziunea APF. Organizațiile și publicațiile de stânga au fost însă destul de critice, apariția publică a „mass-mediei de stat", care este planificată să fie utilizată în timpul unei crize informaționale, nefiind agreată în aceste cercuri. În timpul exercițiului au fost utilizate stații radio mobile, televiziunea a operat din locații fixe, iar detașamentele de presă au folosit instalații civile (de cele mai multe ori în timpul nopții). De la acest exercițiu, APF nu a mai desfășurat activități într-un mod așa public și după câțiva ani s-a reorganizat în regimentul informațional.

Pentru cazuri speciale, Bundesrat-ul are la dispoziția sa un comandament separat (Stab Bundesrat, Abteilung Presse und Funkspruch - Stab BR APF) pentru a informa populația. Responsabil pentru acest departament de presă și radio este tot departamentul de justiție și poliție. Acțiunile acestui comandament se desfășoară

în cazul în care instituțiile civile nu mai sunt în stare (parțial sau total) să ducă la îndeplinire sarcinile lor de informare.

Încrederea reprezintă prinicipiul de bază al acestor activități. Doar o politică credibilă de informare poate menține încrederea în conducerea politică și militară. Informația trebuie să fie precisă, relevantă și pe înțeles. Datorită principiului de încredere pe care îl promovează, acest comandament nu este un instrument de război psihologic.

Comandamentul are un consiliu de conducere al cărui președinte este secretarul general al departamentului de justitie și poliție. Un organism subordonat (Politisch Publizitsche Leitung - PPL) este responsabil pentru consilierea pe linie de informații a guvernului. Regimentul 1 informațional conduce activitățile mass-media și realizează transmisiunile radio și TV.

Regimentul 1 informațional are structura sa de astăzi începând din 1 ianuarie 1997. Constă dintr-un stat major și cinci „Abteilunge", comparabile ca nivel cu batalionul. Unul este pentru sprijinul statului major, iar celelalte (numerotate 10, 20, 30 și 40) sunt elemente operaționale. „Input-Abteilung 10" (trei companii) este responsabil pentru obținerea și procesarea informațiilor cu ajutorul unor specialiști în limbi străine.

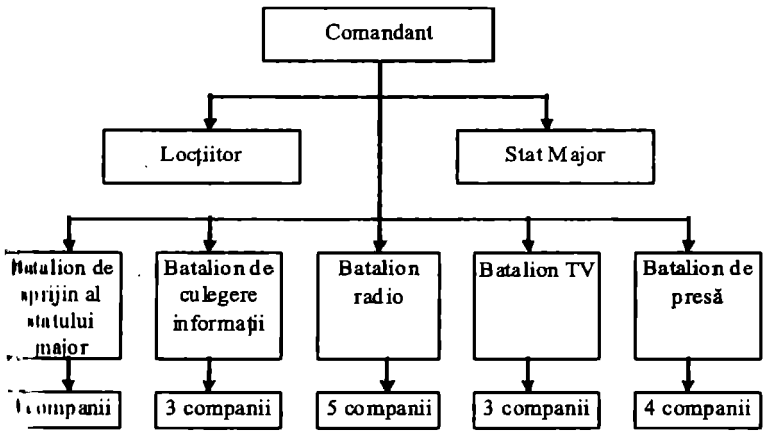


Figura 2. Organizarea regimentului 1 informațional

„Radio-Abteilung 20" are cinci companii radio care au misiunea de a asigura că guvernul și comanda militară pot informa rapid populația pe întreg cuprinsul țării. Stații radio FM foarte puternice, răspândite pe întreg cuprinsul țării, transmit programe în trei limbi care pot fi auzite chiar și în adaposturi de nivel 3. Informația poate fi transmisă și în limbi străine pentru anumite grupuri din țară sau exterior.

„TV - Abteilung 30" are trei companii TV și poate să transmită programe de urgență în trei limbi, prin aceasta răspândind mesajele și directivele autorităților regionale și naționale.

Companiile radio și TV pot funcționa din locații subterane amenajate și dispun și de stații mobile.

„Press -Abteilung 40" produce ziare, foi volante și afișe în cele trei limbi. Aceste produse sunt distribuite din locuri speciale spre populație, militari și unitățile civile pentru starea de urgență. Companiile și detașamentele utilizează instalațiile de tipărire de pe întregul Elveției. În acest moment, regimentul numără 1640 de militari. Mulți dintre ei sunt activi în domeniul mass-mediei civile și toți au pregătire militară de bază. Viitoarele progrese tehnologice vor putea permite ca numărul personalului să scadă cu aproape 1000.

Pentru acest regiment, regulile militare din armată nu se aplică în totalitate. În fiecare an ofițerii și soldații au câteva zile (7 -10) de serviciu activ. Un soldat poate fi în serviciu cel mult 300 de zile și până la vârsta de 40 de ani. Ofițerii și comandanții pot servi mai multe zile. În cazul unei crize, Bundesrat-ul decide cât personal este necesar. În cazul unei catastrofe, detașamentele pot fi activate imediat pentru unele misiuni speciale.

Pentru transmisii radio, detașamentele pot fi gata de acțiune în câteva ore. Antrenamentul în vederea misiunilor reale constă din exerciții de verificare a starii de pregătire după mobilizare în condiții dificile.

Statul major, elementele de comandă și „soldații mass-media" sunt pregătiți în diferite scenarii de criză o dată la doi ani. În 1997,

de exemplu, exercițiul „Alpha" a inclus elemente ale statului major și „Input Abteilung 10". Antrenamentul a cuprins „Radio-Abteilung 20", cu două dintre companii, și „Presse - Abteilung 40", cu elemente din toate cele patru companii.

Exercițiul a durat 72 de ore și s-a bazat pe o serie de evoluții ipotetice în Balcani, „situație" în care regimentul trebuie să sprijine mass-media rămasă. Prin utilizarea de noi transmițători, noi tehnologii și mașini de tipărit, exercițiul a dovedit că experiența și cunoștintele de specialitate sunt vitale.

SIGURANȚA INFORMAȚIONALĂ

ERIC LUIIJF M.SC.ENG.*

Tehnologia Informației și Comunicației (ICT- *Information and Comunication Technology)* are un impact imens asupra modului de desfășurare al operațiunilor militare. Forțele armate moderne utilizează pe scară largă hardware și software comercial. Structurile militare și guvernamentale de luare a deciziei, industriile critice și societatea în ansamblu devin tot mai mult interconectate în rețele. Ele se bazează pe infrastructuri fundamentale, globale, convergente și complicate.

Cele mai multe din aceste infrastructuri sunt controlate de elemente ICT complexe. Atât sistemele de comandă-control militare precum și activitatea curentă devine tot mai dependentă de infrastructurile informaționale.

Siguranța informațională, ca parte a operațiilor informaționale defensive, are ca obiectiv protejarea atât a posturii de securitate specifice forțelor armate cât și a infrastructurilor informaționale de bază.

Lucrarea abordează aspectele militare și civile ale siguranței informaționale. Ea oferă cititorului o vedere de ansamblu asupra amenințărilor clare și prezente specifice cyber-spațiului pentru forțele armate și întreaga societate. Este prezentată o taxonomie a cyber-atacurilor structurate atât după metodele de hacking cât și după motivul atacului.

Lucrarea discută importanța ce trebuie acordată siguranței informaționale și concluzionează cu o listă de probleme nerezolvate la nivel internațional.

* Laboratorul de fizică-electronică, Olanda.

Nu cu mult timp în urmă, războiul în cyber-spatiu, trăgătorii automați, muniția inteligentă și armele de mare putere energetică au existat numai în literatura de ficțiune și filme cum ar fi Star Wars (luptătorii stelari).

În zilele noastre operațiile informaționale (Info Ops) au trecut de la gândirea conceptuală la realitate și au devenit un subiect fierbinte atât pentru militari cât și pentru guverne.

In ultimele două decenii, ICT a avut un impact important în modul de desfășurare al operațiunilor militare. În același timp, Departamentul Apărării nu mai este factorul principal în evoluțiile din domeniul ICT.

Forțele armate moderne utilizează pe scară largă hardware și software comercial. De asemenea, structurile militare și guvernamentale de luare a deciziei, organizațiile, societatea și industriile critice devin tot mai mult interconectate în rețele. Pentru funcțiile de bază ele se axează pe infrastructuri globale, convergente, complicate și adesea publice.

Multe din aceste infrastructuri sunt controlate de sisteme ICT complexe. Atât sistemele militare de comandă-control cât și întreaga societate și în special „societatea vestică" - au devenit foarte dependente de infrastructura informațională și este nevoie de o abordare atentă a amenințărilor asociate.

Aproape zilnic hackerii explorează vulnerabilitățile infrastructurilor noastre globale ICT și ale sistemelor de calcul din acestea. Până acum adversarii ideologici și culturali, cum ar fi indivizii, grupurile de guerillă și grupurile teroriste nu au descoperit complet „războiul informațional", ca un mijloc important de a afecta atât operațiile militare cât și societatea.

Distrugerea fizică prin intermediul bombelor și uciderea oamenilor prin intermediul atacurilor teroriste reprezintă încă acțiunile preferate mai mult decât acțiunile în cyber-spatiu. Totuși, unele activități au identificat deja mijloacele omului sărac de a face astfel de lucruri. Atât timp cât rămâne ascunsă în a patra dimensiune, info-sfera păstrează o distanță sigură în timp și spațiu.

Forțele armate, guvernele și societatea în ansamblu trebuie să se pregătească pentru a face față noilor amenințări la adresa infrastructurii informaționale. Totuși, lipsa curentă de conștientizare despre securitatea informațională și vulnerabilitățile infrastructurii informaționale dau naștere la teama că pericolul clar și prezent al cyber-amenințărilor nu este luat în serios.

Siguranța informațională, ca parte a operațiilor informaționale defensive are ca obiectiv protejarea atât a posturii de securitatea informațiilor deținute de forțele armate cât și a infrastructurilor informaționale de bază.

Aceasta lucrare abordează atât aspectele militare cât și civile ale siguranței informaționale. Este prezentată o taxonomie a cyber-atacurilor și a atacatorilor și o viziune introductivă despre hacking și tehnicile specifice. Lucrarea concluzionează cu o listă de probleme nerezolvate la nivel internațional.

MC422 al NATO „Politica operațiilor informaționale" definește operațiile informaționale ca: *„Acțiuni desfășurate pentru a influența factorii de decizie în sprijinul îndeplinirii obiectivelor politice și militare prin afectarea informațiilor celuilalt, a proceselor bazate pe informații, a sistemelor de comandă-control și a sistemelor de informare și conducere în același timp cu exploatarea și protecția propriilor informații și/sau sisteme informaționale".* Există două categorii principale de operații informaționale: defensive și ofensive, depinzând de natura acțiunilor implicate.

Termenul de „Siguranță informațională" a fost introdus de forțele armate ale SUA, pentru a desemna protecția informațională a bunurilor proprii și se definește ca: *„Operații informaționale care protejează și apără informația și sistemele informaționale prin asigurarea pentru ele a disponibilității, integrității, autenticității, confidenfialității și non-repudierii".* Aceasta include facilități de restaurare a sistemelor informaționale prin încorporarea de capabilități de protecție, detecție și reacție.

Eu văd această definiție inadecvată din câteva motive. Mai întâi de toate definiția SUA ia în considerare o listă incompletă de aspecte de securitate informațională, ea neglijează de exemplu aspectele de securitate, cum sunt credibilitatea, supraviețuirea, siguranța și auditul (verificarea de control).

În al doilea rând această definiție neglijează protecția infrastructurilor critice și de bază, care este necesară pentru libertatea politico-militară de a acționa și decide. Infrastructurile sunt în zilele noastre globale, îngemănate, și cel mai adesea controlate de companii comerciale.

Pentru a acoperi toate aceste aspecte, eu propun următoarea definiție de nivel înalt pentru siguranța informațională: *„Siguranța informațională reprezintă acțiunile desfășurate pentru a proteja statul/uniunea, societatea, aliații internaționali, interesele economice naționale și internaționale împotriva atacurilor și disturbanțelor informaționale din sistemele informaționale, infrastructurile informaționale, procesele bazate pe informații și infrastructurile informaționale de bază și servicii".*

Definiția ia în considerare toate capacitățile informaționale civile și infrastructurile critice ale unei națiuni sau ale unei entități economice cum ar fi Uniunea Europeană și aliații ei. Desigur, siguranța informațională nu poate și nu ar trebui să se oprească la granița țărilor.

Mai mult, siguranța informațională ar trebui să se bazeze pe acordul de sprijin mutual între țări și uniuni. Se poate argumenta că definiția de mai sus pentru siguranța informațională ar trebui să fie „fără stat", ca autostrada informațională ce traversează multe granițe de țări. Statul sau uniunea este cea mai înaltă structură organizațională care poate trata la nivel național și internațional vulnerabilitățile societății informaționale în extensia lor, de la disfuncționalități ale serviciilor bazate pe autostrada informațională la operații informaționale psihologice (Psy Ops).

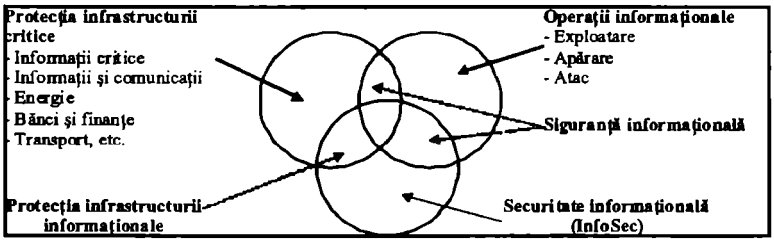


Figura 1: *Legătura dintre siguranța informațională, operațiile informaționale, securitatea informațională și protecția infrastructurii informaționale*

Figura 1 evidențiază legătura dintre siguranța informațională, operațiile informaționale, securitatea informațională și protecția infrastructurii informaționale.

În mod curent, forțele armate, structurile guvernamentale și industriile critice devin tot mai mult interconectate în rețele și se bazează pe infrastructuri îngemănate și convergente. Ca un exemplu, peste 95% din comunicațiile forțelor armate ale SUA pe timpul operației Furtună în Deșert s-au purtat pe linii și sateliți închiriați.

Cele mai multe dintre aceste infrastructuri informaționale sunt controlate de elemente ICT complexe. Structurile de bază pentru aceste infrastructuri sunt totuși aceleași echipamente hardware și produse software comerciale care sunt utilizate peste tot în lume. Cunoștințe și programe despre exploatarea vulnerabilităților specifice echipamentelor hardware și produselor software comerciale pot fi achiziționate cu ușurință. O vulnerabilitate găsită de un hacker seara devreme, în Australia, ar putea să devină cunoștințe uzuale în alte părți ale lumii aproape cu viteza luminii. Cu alte cuvinte, sistemele din Europa și SUA pot fi deja atacate la sfârșitul zilei sau chiar pe timpul nopții corespunzător timpului local.

Una dintre misiunile forțelor armate ale unei națiuni este să prevină atacurile posibile la adresa națiunii și să apere națiunea în cazul unui atac al adversarului. Întrebarea este ce rol vor avea

forțele armate pentru a realiza apărarea națiunii în cyber-spatiu. Este nevoie să fie luat în considerare că cyber-spatiul se extinde dincolo de granițele legale internaționale și depășește cu mult spațiul de luptă militar în dimensiuni de teren, mare și aer.

Mai mult, în contextul conflictelor militare posibile, există o probabilitate sporită pentru conflicte de tip asimetric și de intensitate redusă în care operațiile informaționale să joace un rol fundamental. Cu toate acestea, ar trebui luat în considerare că amenințările nu sunt locale unui „teatru" al operațiilor, dar pot să-și aibă originea de la oricare adversar oriunde în afara societății globale și pot să se întâmple oricând în cyber-spațiu.

Cyber-teroristul este o persoană ce acționează premeditat, o organizație non-militară motivată politic, un grup subnațional, un agent clandestin sau un grup de acțiune sau susținătorii lor care dispun de posibilitatea unor amenințări neconvenționale la adresa unui spectru larg de ținte militare și non-militare, inclusiv baza economică.

Într-o perioadă scurtă de timp ei pot genera atacuri împotriva societăților din noua generație informațională. Afectarea infrastructurii informaționale a unei singure națiuni, de exemplu, membră a unei alianțe ar putea împiedica, sau chiar opri acțiunile forțelor armate ale întregii alianțe.

Când abordăm latura defensivă, se poate concluziona că forțele armate și societățile bazate pe ICT sunt pregătite pentru tratarea noilor amenințări globale. Deși tehnologia de informații și comunicații de nivel performant este necesară, succesul în atacarea bazelor și infrastructurilor informaționale critice nu necesită investiții majore și sunt ușor realizabile de către adversarii potențiali.

Multe unelte sofisticate și de ajutor precum și documentația pot fi aduse gratuit de pe Internet, iar șansele de a fi identificat sunt reduse. În concluzie, este necesar un nivel sporit de siguranță informațională pentru a face față acestor amenințări.

În ciuda multor semnale de avertisment din partea hacker-ilor, cailor troieni (ex. Back Orifice și NetBus) căderilor de tensiune și

firelor arse, precum și conștientizării problemei de tip Y2K, atât forțele armate cât și societatea erei informaționale par să nu dorească investigarea și cercetarea vulnerabilităților lor și să întreprindă în consecință măsurile corespunzătoare.

Deși forțele armate din câteva națiuni se ocupă de operații informaționale, este adesea trecută cu vederea protecția bunurilor și infrastructurilor de management de urgență ale guvernului pentru a fi utilizate de către agențiile guvernamentale și forțele armate. Cu excepția unui număr redus de națiuni, nu este luată în serios continuitatea și protecția infrastructurilor informaționale și sistemelor informaționale de bază. Acele națiuni care întreprind unele acțiuni, înțeleg că ele au de-a face cu o sarcină serioasă care ar trebui să fie îndeplinită în cooperare cu Departamentul Apărării, agențiile guvernamentale și prin colaborări publice-private. De asemenea, aspectele legale și regulile existente interzic un curs al acțiunilor „gata de luptă".

Ca un exemplu, președintele Comisiei de Protecție a Infrastructurii Critice (PCCIP) din SUA are în vedere vulnerabilitățile din următoarele domenii: informații și comunicații, energie (sisteme de tensiune electrică), transport și stocare de gaze și petrol, bancar și financiar, transport fizic (incluzând controlul traficului aerian) și servicii umane vitale. PCCIP a raportat că există o dependență sporită de infrastructurile critice.

Dezvoltările tehnologiei de calcul și îmbunătățirile în ritm amețitor au generat apariția erei informaționale și afectează aproape toate aspectele de comerț și societate. Securitatea noastră, economia, modul de viață și poate chiar supraviețuirea sunt acum dependente de acest trio inter-relaționat al energiei electrice, comunicațiilor și calculatoarelor. Inter-legăturile infrastructurilor sunt, pe puțin spus îngrijorătoare. Oricine prevede ce este mai rău dacă cel puțin una dintre infrastructuri este afectată, fie deliberat fie ca „voință a Domnului".

„Capabilitățile de a lansa un atac împotriva infrastructurii informaționale a unei națiuni sunt acum foarte răspândite și un

atac probabil nu este foarte departe" avertiza Philip La Combe, președintele PCCIP. Afectarea serviciilor de care economia și bunăstarea noastră depind, ar putea avea efecte semnificative și dacă se întâmplă frecvent ar putea afecta serios confidențialitatea publică.

PCCIP a concluzionat că sporirea vulnerabilităților cuprinde amenințările clasice asupra infrastructurilor precum și noile cyber-amenințări. Comanda corect transmisă pe o rețea la un calculator de control al unei stații de generare a tensiunii electrice ar putea fi comparabilă cu efectul unei încărcături de exploziv. Infractorul ar fi greu de depistat și reținut. Mai mult, infrastructurile cresc în complexitate și sunt operate aproape de capacitatea lor proiectată.

Aceasta sporește probabilitatea efectelor în cascadă ce încep chiar cu o distorsiune minoră și de rutină și se încheie numai după afectarea unei mari regiuni. Din cauza complexității lor tehnice, unele dintre aceste dependențe nu pot fi cunoscute până când apare o eroare majoră. Această eroare poate fi introdusă fie de o greșeală operațională, o eroare tehnică, un act de sabotaj - sau un act de „cybortage".

Deși infrastructurile au fost întotdeauna ținte atractive, națiunile vecine, prietene și de graniță au realizat în trecut elemente de protecție. Astăzi această situație s-a schimbat dramatic deoarece granițele naționale nu mai sunt relevante în cyber-spațiu. Atacurile serioase posibile în cyber-spațiu pot fi concepute și planificate fără o pregătire logistică detectabilă.

Ele pot realiza cercetarea invizibil, se pot repeta clandestin, și apoi pot fi planificate în intervale de minute sau chiar secunde, fără dezvăluirea identității și locației atacatorului. Deoarece Forțele Armate utilizează pe scară largă aceleași infrastructuri, devine tot mai dificil să se facă o distincție între atacuri la adresa forțelor armate și cele la adresa societății.

Aproape zilnic se poate citi în ziare despre exemple de vulnerabilități ICT ale societății „vestice" și despre modul cum Forțele Armate și societatea se ocupă de ele. Oamenii par să

zâmbească la aceste incidente și uită despre impactul care ar putea să apară când sistemele informaționale și infrastructura sunt vizate deliberat pe scară largă.

Văzut în această lumină este necesar să revedem câteva exemple.

Lecțiile învățate din disfuncționalități datorate dezastrelor naturale, de exemplu cutremurul Hansin-Dai-Shinsai, din 17 ianuarie 1995, cu epicentrul aproape de Kobe. Vulnerabilitatea societății noastre bazate pe ICT a fost demonstrată în multe moduri. Deși a existat suficientă hrană disponibilă, ea nu a putut fi vândută deoarece sistemul de comunicație ATM a fost afectat cauzând o lipsă de bani lichizi.

Sistemul de comunicații de urgență de rezervă prin intermediul sateliților a fost afectat deoarece cutremurul a deplasat antenele de recepție la sol și nimeni din zona de dezastru nu știa cum să le realinieze.

Cutremurul din 1995, din zona Golfului San Francisco, a evidențiat același tip de vulnerabilitate ICT.

După învățămintele haosului pieței financiare cauzat de explozia unei bombe în Piața Londrei, pe 4 noiembrie 1992, reprezentanții IRA au utilizat apeluri anonime pentru a afecta infrastructura serviciilor (ex. zona financiară din Londra). Ei au planificat de asemenea să plaseze fie bombe reale, fie bombe care par a fi reale, la șase substații de electricitate din afara „inelului de oțel" de securitate al Londrei.

Dacă planul ar fi avut succes, companiile de deservire implicate ar fi închis ele însele întreaga alimentare cu energie electrică într-un mod controlat. Aceasta pentru a reduce șansele de cădere în cascadă a circuitelor electrice în întregul Regat Unit. A fost estimat că ar fi fost afectate toate serviciile de alimentare cu energie din Londra pentru cel puțin 1-1,5 zile. Haosul și efectele psihologice ar fi fost impresionante. PIRA nu a înțeles (încă) că transmiterea comenzii corecte la elementul de control la distanță al liniilor de tensiune dă naștere la același efect.

Fanii fotbalului în încercarea de a obține bilete pentru Cupa Mondială de fotbal din 1998 au determinat colapsul rețelelor telefonice în câteva țări ale Europei, în 22 aprilie 1998. Numai în Olanda, 30 de oficii telefonice centrale au căzut în câteva ore. Aceasta a inclus patru orașe importante și numerele de urgență corespunzătoare. La fel ca Rinus Michels, primul antrenor de fotbal, eu am concluzionat *„Fotbalul reprezintă o infrastructură de război".*

Automatele de vânzare se presupune că apelează compania de distribuție când devin aproape goale. Totuși, unele dintre mașinile incorect instalate din Australia au apelat numărul implicit 000, care este numărul de urgență din Australia. Deoarece au existăt mii de mașini instalate, aproape 1 milion de apeluri „greșite" pe an au făcut serviciul de urgență să blocheze accesul pentru cele ce necesitau intervenția cu adevărat. Aceste tipuri de „atacuri" larg răspândite par să fie greu de gestionat.

Pe 10 martie 1997, un hacker tânăr a închis comutatorul oficiului central al companiei Bell Atlantic din Worcester aproape de Boston, SUA. Ca rezultat aeroportul a pierdut serviciile telefonice și de date pentru mai bine de 6 ore. Pe 4 ianuarie 1999, cinci indivizi au pătruns într-un oficiu telefonic din Las Vegas Sprint și au oprit echipamentele de comutare telefonică. Aceasta a determinat 7 ore de întrerupere a serviciului telefonic pentru 75.000 de clienți.

Pe 19 mai 1997, satelitul PanAmSat Galaxy IV a fost scăpat de sub control, întrerupând serviciul de pager pe perioada a 3 zile, pentru 80-90% din 40 de milioane de pagere utilizate în SUA. Doctorii au fost printre primii afectați, deoarece spitalele le făceau apeluri în caz de urgență, precum și ofițerii de poliție.

Amsterdam Internet Exchange a căzut pe 26 decembrie 1998 datorită unei defecțiuni a transformatorului de tensiune electrică. Olanda a fost efectiv tăiată de la Internet pentru un număr de ore. Pe 16 iunie 1999, 4 fire au fost tăiate la Groningen, determinând oprire instantanee a serviciilor mobile și fixe precum și pierderea serviciilor de date în provinciile nordice ale Olandei.

Pe 26 martie 1999, macro-viermele Melissa s-a răspândit foarte rapid pe Internet. Multe site-uri guvernamentale ale SUA incluzând baza militară ce susținea operația din Kosovo au apărut a fi vulnerabile. Din fericire, viermele nu a avut „efecte" distructive.

Din aceste cauze și multe altele, din faptul că aproape zilnic se înregistrează incidente grave ar trebui să fie clar că forțele armate, guvernul, societatea, organizațiile și industriile critice trebuie să se pregătească împreună pentru apărarea bunurilor lor în era informațională.

Cyber-atacurile și cyber-terorismul pot fi găsite pe harta rutieră specifică operațiilor informaționale. Întrebarea este dacă cineva ar putea privi asta ca o amenințare a viitorului, o amenințare futuristă sau ca o amenințare a zilelor noastre. Este ea reală sau este ficțiune? În studierea acestei probleme, bazele de informații deschise nu prea oferă fapte substanțiale.

De exemplu, infracțiunile în domeniul calculatoarelor nu sunt înregistrate ca un element distinct de către cele mai multe birouri de statistică. Ele vor fi probabil clasificate drept infracțiuni cum ar fi furtul, falsificarea sau altă categorie. Astfel nici o abordare sociologică a cyber-atacurilor nu este la îndemână. Infractorii se află de la copii de școală, studenți, oameni bolnavi mintal care trăiesc izolați de societate până la teroriști reali.

Unele grupuri de hackeri ex. *Master of Downloading* (MOD) au membri multinaționali. Pe de altă parte, terorismul însuși va rămâne o problemă trans-națională, condusă de minoritatea etnică, religioasă, naționalistă, separatistă, politică și motivații economice. Cyber-terorismul este gata să apară în toată măreția lui cât de curând. Pentru a răspunde întrebării *„Cyber-atacul: fapt sau ficțiune?"* trebuie să facem o evaluare in vederea clasificării diferitelor aspecte legate de acestea.

Când sunt evaluate diferite tipuri de conflicte care ar putea să apară, ar trebui avut în vedere tipul și intenția adversarilor potențiali. Tabelul I, potrivit lui Waltz furnizează o astfel de abordare.

Războaie de gherilă

		Nivel tehnic ridicat	Nivel tehnic redus
	Conflict fizic	**1. Război de comandă-control** -câmp de luptă de înaltă intensitate -presiune și putere economică -țintă: precisă -consecința: fizică -tehnologia C4I	**3. Război de gherilă** -câmp de luptă de intensitate mică -cruzime -ținte aleatoare -consecința: mediul natural -rețele umane (și tehnologice)
Războaie pe baze economice	Conflict abstract	**2 Război în rețele, cyber-război** -conflictul în cyber-spațiu -cunoștințe și putere -țintă: baza de informații -consecința: utilizarea ITC - rețele globale și tehnologice	**4 Război, conflict și putere ideologică** - țintă: masele/ societatea - consecința: ideologică - rețele umane ideologice

Terorism

Războaie culturale

Tabelul 1. Tipologia a patru tipuri de conflict

Este clar că accentul important în dreptunghiul 1 revine componentei militare (operații informaționale; războiul de comandă-control). Cyber-teroristul de înalt nivel tehnic (dreptunghiul 2 în figură) - un individ premeditat, o organizație militară motivată politic, un grup sub-național, un agent clandestin, sau un grup de acțiune - sau suporterii lor care au posibilitatea generării unor amenințări neconvenționale la adresa unui spectru larg de ținte militare și ne-militare, incluzând baza economică.

Un avantaj major pentru protagonistul virtual (dreptunghiul 3 și 4) este că acesta nu este nevoie să se găsească în preajma, în timp sau spațial când se realizează atacul sistemului sau infrastructurii. Pregătirea unui atac întârziat este ușoară deoarece modemul de comunicare pentru lansarea atacului poate fi ușor programat automat.

Infrastructura globală face ușoară alegerea unei țări din care atacul este pregătit și la fel este ușor de ascuns utilizarea liniilor telefonice internaționale pentru a ajunge la un modem în altă țară. Pentru securitatea serviciilor, guvernului și organizațiilor atacate le va fi greu să aibă indicii asupra țintelor care ar trebui selectate. Lipsind această informație, va fi greu de găsit timpul necesar avertizării. Urmărirea și indentificarea grupurilor teroriste virtuale va fi chiar dificilă dacă nu imposibilă.

Posibilitatea de a utiliza aceste aspecte ca mijloace tehnice, utilizând tehnologii noi și combinate, face situația diferită în raport cu mijloacele de război existente înainte. Costul relativ redus, rata de succes posibil ridicată și probabilitatea de a o deține, fac în principiu „Operațiile informaționale ofensive" atractive pentru indivizi, adversari economici, precum și pentru grupurile de protest și teroriste.

Prima abordare este de a vedea tipurile de preocupări de hacking în cadrul tabloului general de hacking.

– **Hackeri** – cei ce vor să pătrundă fraudulos pentru a demonstra vulnerabilitatea sistemelor de calcul și a rețelelor prin

exploatarea sistemelor administrate „mai puțin bine" și/sau a punctelor slabe cunoscute. Intenția lor nu este de cele mai multe ori una distructivă, dar generează o întrebare de genul „Ce va fi dacă...?" Acestea includ strănuturi și sughițuri la adresa celor ce ascultă pe rețele pentru parole simple.

• **Crackeri** – cei ce pătrund în sistemele de calcul, încercând să distrugă sau să modifice informații sau să exploateze aceste sisteme ex. distribuirea ilegală de software. Crackerii software sunt specialiști în acest grup care sparg verificările de securitate/ identitate ale pachetelor software.

• **Phreakeri** (anomalii telefonice), expoatează schimburile telefonice, sistemul telefonic celular și utilizarea semnalului telefonic pentru fraudă. Ei, de asemenea, pot fi implicați în frauda de cartele inteligente și cărți de credit. Grupul phreak-erilor „Specialiștii în telefoane" au pătruns la comutatoarele AT&T, Southern Bell, BT, au avut acces la porțiuni din rețeaua de electricitate a SUA și la sistemele de control a traficului aerian. Ei au redirecționat liniile telefonice ale FBI înspre liniile telefonice pentru discuții de sex din Germania și alte țări și au obținut acces la listele de linii telefonice ascultate (în final a reieșit că însăși liniile lor telefonice erau monitorizate de FBI).

• **Socio-ingineri**, cei ce sunt culegători de informație de nemulțumire, ceea ce le permite să culeagă parole sau alte informații vitale pentru a accesa sistemele și rețelele. **Thrash**-erii (bătăuși) sunt socio-ingineri ce utilizează metode de culegere fizică a informațiilor. Așa numiții **dumpster-divers** (scafandrii în gunoaie) care umblă prin gunoaiele companiei pentru a găsi informații valoroase ce pot să-i ajute să pregătească un atac socio-inginerese sau să atace direct.

• **Hackeri pentru modemuri de cablu TV, comunicare prin satelit și de plătire a taxelor TV**, sunt cei care sparg sistemul de codificare al semnalului TV în scopul de a vedea transmisiunile gratuit. Acțiunile lor curente au numai impact economic. Prin

oferirea posibilității de acces Internet prin intermediul modemurilor de cablu CATV, amenințările la adresa confidențialității, integrității și securității devin o problemă. Totuși acestea sunt clasificate în alte categorii.

• **VX**, creatori de viruși, indivizi ce scriu programe virus și le lansează în acțiune. Așa numiții *„lamers"* sunt de clasă mai slabă „ei utilizează chituri de construcție pentru viruși, fac mici modificări nefolositoare sau doar infectează calculatoarele altora...

• **Screen droppers** (culegători de ecran), monitorizează de la distanță, pe ascuns, ecranele calculatoarelor utilizând radiația electromagnetică a ecranelor. Aceste sisteme ar putea culege informația de pe ecran de la o distanță de 1 km. Măsurătorile cu Standardul de Emanație a Pulsului Electromagnetic Tranzient (TEMPEST) reduc considerabil expunerea la acest risc.

• **Utilizatorul intern**: poate fi oricare dintre cei de mai sus care poate avea acces „nelimitat" la informația și sistemele interne.

În al doilea rând am putea ordona cyber-atacurile pe baza motivelor atacurilor și în funcție de cine este în spatele acestor atribuțuni.

• **Incompetența, neglijența.** *Subiectul:* utilizatorul intern. *Scopul:* evident fără scop. De observat că tot ce a fost spus despre hack-erul extern ar trebui pus în balanță cu rezultatele mai multor studii ce arată că utilizatorul intern este responsabil pentru 60%-80% dintre breșele existente în securitatea informației. Lipsa de apărare datorată neglijenței și lipsa de conștientizare a securității este cauza principală a atacurilor cu succes. Cei din afară pot ataca adesea prin utilizarea căilor lăsate neblocate de către administratorii de sistem și de rețea. Mai mult, orice organizație ia măsuri importante pentru a determina activitățile neautorizate ale utilizatorilor interni.

• **Interzicerea (refuzul) intern de serviciu.** *Subiectul:* angajatul nemulțumit care vrea să-și răneasscă șeful. *Scopul:* resturi arse (informații șterse sau stricate) sau informații blocate (cheia cunoscută numai de șef).

• **Hacking de recreație/amator.** *Subiectul:* Un singur individ sau un grup restrâns de adolescenți, studenți și persoane interesate tehnologic, uneori lucrând în grupuri similare (egale). *Scopul*: Încercarea de a înțelege ICT și calea prin care uneori sau adesea sistemele de securitate nu funcționează (curiozitate). *Riscul limită:* persoana poate deveni un „mic criminal" prin obținerea de rezultate financiare (ex. phreaking, fraudă de cartele inteligente).

• **Nesupunere electronică.** *Subiectul:* grupuri de activitate, suporterii unei cauze. *Scop:* obținerea atenției mijloacelor de informare și întreruperi temporare ale serviciilor prin atacuri de interzicere a serviciului. *Riscul limită*: să devină mai violent când acțiunile nu au impactul scontat. De exemplu: Teatrul de Disturbanță Electronic în sprijinul mexicanului Zapatista a invadat serverele web ale președintelui mexican, Biroul de Schimb al Stocurilor din Frankfurt și Departamentul Apărării al SUA cu cereri de pagini web. Rezultatul a fost interzicerea serviciului pentru ceilalți utilizatori.

• **Hacking pentru căutare de publicitate.** *Subiectul:* Un singur individ sau un grup restrâns de adolescenți, studenți și persoane interesate tehnologic precum și un grup de hackeri (semi) profesionali. *Scopul:* intenția de a obține o atenție sporită în mijloacele de informare prin pătrunderea într-un sistem ICT important și comentarea acestui fapt. *Riscul limită*: să devină implicați/angajați de criminali sau grupuri sub-naționale.

• **Căutător de suport legal.** *Subiectul:* Persoana sau grup de hacking semi-profesional; angajat nemulțumit de șeful „direct". *Scopul:* încercarea de a discredita un serviciu ICT și/ sau serviciu de deservire, pentru a-și dovedi propria inocență. *Riscul limită:* a deveni „violent" încercând să impună propriul punct de vedere.

• **Obținerea de informații.** *Subiectul:* Comunitățile de intelligence naționale, culegătorii de informații economice (firmele de intelligence în afaceri), spionaj economic și industrial și persoane/ grupuri profesionale de hacking. *Scopul:* serviciile de

informații naționale și de afaceri, pentru a obține un avantaj față de alte națiuni și organizații.

• **Grupuri de acțiune pentru o cauză;** protagoniști criminali („hack-iviști"). *Subiectul:* Orice grup motivat cu cunoștințe sau pregătire tehnologică. *Scop:* căutarea de publicitate și încercarea de a enerva organizația, departamentul guvernamental sau agenția în discuție. *Mijloace*: urmărirea de atacuri de interzicere a serviciului ex. prin depășiri de memorie, precum și pierderea de integritate a sistemelor. *Riscul limită:* a deveni „violent" în încercarea de a face cunoscut punctul lor de vedere și deplasarea înspre terorism.

Ca un exemplu, în august 1999, câștigătorul premiului NOBEL pentru pace din 1996, Jose Ramos-Horta a amenințat guvernul indonezian. Un grup de peste 100 de hackeri din întreaga lume au simpatizat cu luptătorii pentru independență din Timorul de Est și erau gata să atace bunurile economice principale ale Indoneziei (bănci, operatori de telecomunicații, linii aeriene), în caz că guvernul indonezian nu accepta rezultatele referendumului ținut în Timorul de Est.

• **Avantaj economic.** *Subiectul:* Un partener de afaceri fără scrupule sau un angajat „flexibil etic". *Scopul:* obținerea de beneficii prin afectarea activităților de ICT ale competitorilor.

• **Vandalism.** *Subiectul:* În principal angajații sau indivizii nemulțumiți. *Scopul:* Atingerea valorilor economice ale unei organizații.

• **Activități criminale.** *Subiectul:* Persoane/ grupuri de hacking profesionale având ele însele scopuri criminale sau angajate de criminali sau grupuri criminale. *Scopul:* Activitatea (dacă e posibil ascunsă) de a obține informații, contra-informații (ex. obținerea, distrugerea, discreditarea informațiilor poliției) pentru a afecta securitatea infrastructurilor pe timpul unei acțiuni planificate sau pentru a obține un avantaj financiar.

• **Cyber-terorism.** *Subiectul:* Grup sub-național premeditat,

motivat politic, agent clandestin, grupuri criminale organizate sau concurenți economici fără scrupule. Ar putea utiliza grupuri sau persoane de hacking profesional plătite. Dacă atacul este străin sau din interior nu se realizează nici o diferență. *Scopul:* Un spectru larg de ținte militare și ne-militare incluzând baza economică.

De reținut din cyber-atacuri că noile mijloace ICT în general și Internet-ul în particular, sunt utilizate ca mijloace de comunicare pentru distribuirea informațiilor sub-naționale, teroriste și criminale (ex. recipiente bombă, curse de prindere prin blocare, oferte de pașapoarte ilegale) și comunicarea secretă. Aceste categorii nu sunt tratate în această lucrare.

Pe lângă erorile generate către utilizatorul intern, cele mai multe cyber-atacuri au propriile lor circuite informaționale subterane (ascunse), uneori chiar în bazele de informații deschise pe web. De exemplu, instrumente phreaker și cunoștințe sunt utilizate pentru a deschide un circuit telefonic.

Hackerii ar putea să treacă prin sisteme de calcul multiple și să se schimbe înainte de a ajunge la ținta lor care ar putea să reprezinte mersul prin țări diferite. Unele grupuri de hacking sunt bine organizate și au propriile lor publicații (ex. 2600 în SUA, care a apărut de mai bine de l0 ani, Clubul Haosului Calculator în Germania). Multe articole pe acest subiect pot fi găsite de asemenea pe WWW.

Hackerii/ phreakerii interschimbă documente cu cunoștintele lor în care se găsesc chiar elemente de proiectare hardware. Uneori managerii de sisteme Unix și Windows/NT cunoscători, utilizează aceste surse pentru obținerea de detalii de profunzime. Cele mai multe documente și baze de date care au deinformații referitoare la vulnerabilitățile unui sistem pot fi găsite pe Web.

Separat de atacurile fizice, diferite tipuri de mijloace de atac informațional variază de la un mod de atac strict software la mijloace în spectrul electro-magnetic. O listă exemplu a acestor mijloace este prezentată mai jos.

• **Virus calculator**: cod care se auto-reproduce când este executat și infectează pe ascuns codul executabil, incluzând macro-codul. Separat de codul reprodus, un virus conține o taxă de încărcare care se poate manifesta prietenos sau distructiv. Virușii sunt secvențe de program nedirijate. Viteza lor de infectare depinde de tipul mecanismului de infectare utilizat. Cu toate că uneori sunt distructivi sau enervanți, virușii sunt cele mai puțin utilizate mijloace pentru operațiile informaționale.

• **Cal troian**: cod ce are ascuns efecte laterale. Web-site-urile bune și frumoase cu cod activ (Java, ActiveX) reprezintă un pericol pentru descărcarea acestui cod sau vizitarea unor astfel de site-uri.

• **Vierme**: cod auto-replicat (multiplicat) ce utilizează funcționalitatea rețelei ex. mecanismele de distribuție e-mail, pentru a se împrăștia. Virusul „Melissa" care s-a împrăștiat aproape instantaneu pe Internet în 1999, a fost un astfel de vierme.

• **Bomba logică și bomba cu ceas**: o porțiune ascunsă de cod care se execută când o condiție certă-filtrată extern ex. timp, ștergerea unui fișier, schimbarea unui web-site extern se realizează.

• **Torpedo logic**: un tip de virus ce încearcă să avanseze către o mulțime de scopuri certe (sigure), având un sistem sau un program pentru livrarea consecințelor sale acolo.

• **Manipularea datelor**: variază de la discreditarea integrității informației la schimbarea biților datelor la video-morfologie în care informația video sau chiar imaginea este manipulată într-un asemenea mod că de exemplu un președinte strânge mâna cuiva pe care nu l-a întâlnit în întreaga viață.

• **Ușa din spate sau ușa trapă**: o portiță în sistem lăsată de programator sau administratorul de sistem permițând utilizatorilor neautorizați să obțină accesul la o parte sau la întreg sistemul.

• **Proiectarea sistem și sisteme de codificare**: pentru fiecare sistem de operare, software rețea, elemente de comutare rețea și echipamente de protecție de graniță (ziduri de foc, gărzi) listele cu vulnerabilități și petece sunt publicate de vânzători și Echipele

de Răspuns de Urgență pentru Calculatoare. De obicei administratorii de sistem nu dispun sau au timp limitat pentru a instala programe petec, în măsura în care această informație dispare. Aceasta are ca rezultat existența porților deschise, bine-cunoscute pentru multe sisteme de producție.

• **Depășirea de memorie**: bombardarea unui sistem cu foarte multe cereri așa încât sistemul nu poate face față fluxului de intrare rezultând un refuz al serviciului pentru utilizatorii autorizați. O unealtă soft ce a fost proiectată pentru situatii de „inundații" este numită *FloodNet* și este produsă de Teatrul de Disturbanță Electronic.

• **Proiectarea circuitelor**: modificarea circuitelor într-un astfel de mod în care circuitul (chipul) conține o ușă prin spate sau o bombă logică.

• **Cutii albastre**: pătrunderea pe linii telefonice și „jocul" cu semnalele electronice.

• **Apelator de război**: O setare software și de comunicare (modem) ce permite apelarea secvențială rapidă a listelor de numere de telefoane în scopul de a detecta modem-uri active sau linii telefonice ce permit „dialogul-după".

• **Mijloace în spectrul electro-magnetic**, unele exemple:

- înregistrarea informației utilizând radiația ecranelor și softul TEMPEST (soft pentru emisii stimulate).

- interferarea cu semnale radio, ex. un sistem de supervizare GSM, precum și cu transmițătorii de mare putere în spectrul de bandă ultra-largă.

- pulsuri electromagnetice, încărcarea și chiar distrugerea circuitelor sistem;

- echipamente bazate pe micro-unde de mare putere.

Pentru a evidenția amenințările cyber-atacurilor, tabelul de mai jos dă o estimare a probabilității țintei prin țintă și motiv. În același timp se arată dacă atacurile validate au fost raportate de către sursele deschise.

CYBER-ATACURI	**Atacuri validate (Septembrie 1999)**	ȚINTE				
		Informația	**Sisteme & Rețele mici**	**Organizația & Industria**	**Guvernul**	**Infra-structura & Societatea**
Incopetență, neglijență	Larg răspândit	Țintă principală	Țintă principală			
Refuzul intern al serviciului	Larg răspândit	Țintă principală	Limitat	Țintă principală		
Hacking de recreere	Larg răspândit	Limitat	Țintă principală			
Nesupunere electronică	Limitat		Țintă	Țintă principală		
Hacking în căutare de publicitate	Larg răspândit	Țintă principală	Limitat			
Căutator de suport legal	Limitat	Țintă principală				

Obținerea de informații economice	Limitat, în creștere rapidă	Țintă principală				
Atac/rezultat economic	Limitat, în creștere rapidă	Țintă principală	Țintă principală	Țintă principală		Limitat
Obținerea de informații naționale	Cunoscut că se întâmplă	Țintă principală		Limitat?	Țintă?	
Grup de acțiune /hackivist	Limitat, în creștere	Limitat	Țintă principală	Țintă principală	Țintă principală	Limitat
Vandalism	Limitat		Țintă principală	Țintă	Țintă	Limitat
Criminali: crimă simplă	Limitat	Țintă principală		Țintă		
Criminali: crimă financiară	La nivel înalt, în creștere rapidă	Țintă principală	Phreak-ing	Țintă		
Crimă organizată	Necunoscut	Țintă principală		Țintă principală	Țintă	
Cyber-terorism	PIRA: limitat				Țintă	Țintă principală
	Limitat	Țintă principală	Țintă	Țintă	Țintă	Țintă principală

Personalului de întreținere din spațiul SUA și Centrul de Război al Sistemelor Navale din San Diego i-a fost cerut să investigheze plângerile utilizatorilor privind imprimarea cu viteză redusă. Hackerii au redirecționat fluxul de imprimare la un server în Rusia, care în final întorcea ieșirea la imprimanta de destinație. Se poate intui ce se putea întâmpla cu rezultatul imprimării.

Pe timpul crizei din Kosovo, au fost raportate din surse ca Serbia și Rusia precum și de la simpatizanți din alte țări atacuri la adresa sistemelor NATO, sistemelor guvernamentale ale SUA și sistemelor de apărare ale partenerilor coaliției. Separat de atacurile de interzicere a serviciului și de dezafectare a site-urilor web au fost făcute încercări de a pătrunde în rețelele apărării.

Astfel, când se discută problema „Cyber-atacuri: fapt sau ficțiune" putem concluziona că toate tipurile de cyber-amenințări au fost realizate într-un mod sau altul. Zilnic, se pot găsi articole în știrile despre sisteme afectate, cărți de credit și infrastructuri afectate. Totuși, atacuri la întreaga scară, cu un impact major asupra forțelor armate și/sau societății nu au fost (încă) realizate.

Infrastructurile informaționale sunt dependente de ICT, îngemănate și inter-relaționate. Ele sunt foarte vulnerabile. În jur de 80% până la 90% din informația necesară pentru apărarea unei națiuni este în zilele noastre deținută de sectorul privat, cu alte cuvinte este în afara controlului guvernamental. Sunt necesare schimbări fundamentale în abordarea siguranței informaționale în societatea secolului XXI. În continuare sunt evidențiate unele dintre problemele deschise.

Organizațiile în general nu acordă suficientă atenție securității informaționale, neglijează avertismentele, nu pot păstra evidența modificărilor semnificative în cadrul mediului rețea și sunt nepregătite pentru lucrurile care ar putea să se întâmple. Sunt chiar convins că multe agenții guvernamentale au sisteme senzitive și rețele ce posedă porți neblocate care așteaptă să fie deschise de către neautorizați.

Industria de obținere a informațiilor electronice economice, atât etică cât și neetică, se extinde rapid. Există indicatori că

obținerea avantajelor financiare prin utilizarea atacurilor economice ne-etice este în creștere, oferind o șansă redusă de detectare. Cât timp va accepta societatea aceste riscuri?

Cele mai multe guverne au deficiențe cu conștientizarea vulnerabilității propriilor lor societăți. Manifestarea internațională a cyber-terorismului poate fi așteptată mai devreme sau mai târziu. Studii precum cele ale PCCIP al SUA nu sunt încă realizate în cele mai multe țări sau sunt împiedicate de lipsa de cooperare cu alte agenții și industrii guvernamentale.

În cyber-spațiu cineva poate ataca fie de peste stradă, fie de undeva din Timbuktu, fapt ce face și mai dificil mersul după cyber-atacatori. Singura soluție este păstrarea permanentă a porților închise, ceea ce înseamnă vigilență continuă. Organizațiile care utilizează pe scară largă mijloace de informații și comunicații, cum ar fi forțele armate, au resurse foarte limitate atât în termeni de calitate (cunoștințe) cât și cantitate (numărul managerilor de sistem).

Este deja dificil de a ține infrastructura informațională în funcțiune pe o bază de zi-cu-zi. Resursele pentru menținerea posturii de securitate sunt nesatisfacătoare. Organizațiile ar trebui să devină conștiente că siguranța informațională ar trebui să se afle pe lista lor de priorități în scopul de a supraviețui operațiilor informaționale ale adversarului. Problema este dacă acțiunile vor fi întreprinse la timp sau va trebui să avem experiența unui „Pearl Harbor electronic".

Pentru soluționarea acestor robleme este necesar un efort legal internațional fundamental de abordare a vulnerabilităților din cyber-spațiu, un cadru legal internațional, cooperarea poliției internaționale, definirea legală a cyber-atacului și a tipurilor de apărări permise împotriva operațiilor informaționale. În mod curent, suportul legal internațional este ineficient datorită procedurilor complexe.

Adversarul pe de altă parte are nevoie numai de secvențe scurte de biți care sunt măsurate în secunde. În al doilea rând,

pregătirea actuală a poliției implică criminali nu teroriști. Cine va apăra țările împotriva cyber-terorismului? Care va fi rolul serviciilor de securitate în secolul XXI, date fiind amenințările de cyber-terorism și terorism la adresa infrastructurilor? Cum ar trebui să fie organizat schimbul de informație intern al statului pentru a lupta împotriva amenințărilor ce traversează granița?

Pregatirea de urgență necesită instruirea și reevaluarea. Siguranța informațională impune forțelor armate, guvernelor și furnizorilor de infrastructuri critice de informații să fie pregătiți pentru administrarea protectivă a acțiunilor în cazul unui atac. Întrebarea este cum să se dezvolte scenarii de reevaluare realiste, considerând în particular aspectele de depășire a granițelor specifice cyber-spațiului.

Tot mai mult, forțele armate și agențiile guvernamentale utilizează activ echipe „Tiger" sau echipe de infiltrare pentru a încerca să pătrundă în propriile lor sisteme senzitive. Există un număr de aspecte legale când se lansează aceste așa numite capabilități de „Echipă Roșie" care este nevoie să fie rezolvate.

Practic siguranța informațională necesită căutarea activă de găuri în apărarea cuiva în combinație cu detectarea intrușilor și instruirea echipelor de răspuns. Când privim aspectele internaționale întrebarea este dacă țările ar trebui să coopereze în activitățile Echipelor Roșii la nivel tehnic. Este necesară o evaluare continuă a infrastructurilor informaționale internaționale.

Există o scăpare curentă a atenției managementului pentru conștientizarea securității informaționale. Întrebarea este cum să înceapă conștientizarea de siguranță informațională de la nivelul corect în Forțele Armate și organizațiile guvernamentale.

O soluție simplă la unele dintre problemele siguranței informaționale este să se interzică toate comunicațiile electronice și schimburile de informații. Pe de altă parte există presiune pentru utilizarea în comun a informațiilor internaționale între coaliții partenere și guverne. Cum să se păstreze confidențialitatea, integritatea și disponibilitatea informației cuiva dacă un grad sigur

de schimb este necesar înainte de obținerea de informații din alte părți? Pentru a opera cu această dilemă, sunt necesare dezvoltări pe mai departe ale siguranței informaționale.

Și la final, dar nu cea din urmă, hacking-ul și phreaking-ul reprezintă o realitate. Totuși cei mai mulți dintre ei sunt hackeri de recreație. Întrebarea este ce unelte de alertare ar trebui dezvoltate pentru a recunoaște „posibilii" spioni, criminali și teroriști în ansamblul zgomotului de fundal.

CONCLUZII

Pentru a supraviețui posibilelor cyber-atacuri din partea teroriștilor virtuali, fie pentru motive ideologice, fie pentru alte motive, este nevoie ca țările, guvernele și organizațiile să fie pregătite. Cyber-atacatorul are avantajul de a fi plasat în timp și spațiu independent de țintă, în timp ce tehnologia necesară este relativ ieftin de obținut.

Siguranța informațională se presupune că este răspunsul la amenințarea asimetrică. Din acest motiv, siguranța informațională care include aspecte de securitatea informațiilor, protecția infrastructurii de informații și operații informaționale defensive, necesită mai multă atenție decât le este acordată în prezent. Lipsa de conștientizare, de management de securitate și analiza corespunzătoare a riscurilor generează mari riscuri neconsiderate.

Utilizarea echipamentelor hardware și software comerciale sporește vulnerabilitățile posibile ale sistemelor și infrastructurilor în situația în care exploatarea vulnerabilităților cunoscute nu sunt înregistrate imediat. Producătorii comerciali nu sunt doritori să adauge mecanisme ce permit siguranța informațională și încrederea. Întrebarea este cum să se mențină încrederea când se utilizează predominant componente comerciale.

Și deoarece lumea ICT (virtuală), conectivitatea globală, infrastructurile convergente și rețelele interconectate traversează multe granițe internaționale, cooperarea internațională efectivă va fi esențială pentru a înregistra atacurile la adresa națiunii sau infrastructurii informaționale de apărare.

Faptul că forțele armate și comunicațiile de management de urgență se bazează parțial sau uneori chiar în mare măsură, până la o treime deținută de infrastructurile civile, reprezintă o mare problemă. Cooperarea internațională se bazează încă pe tehnologia antică cu factori poștali și procedurile administrative sunt lungi dacă nu chiar birocratice.

Cyber-atacatorul, pe de altă parte utilizează autostrada electronică cu viteza luminii și este informal organizat. Este încă un drum lung de parcurs pentru a acoperi golul pe care îl reprezintă siguranța informațională. Aceasta necesită atât sporirea conștientizării la cele mai înalte nivele de luare a deciziei, dezvoltări tehnologice majore și cooperarea globală pentru sisteme legale armonizate și suport pentru investigarea criminalității.

EXPLOZIA TEHNOLOGIEI INFORMAȚIEI

MAX V. METSELAAR*

Este acceptat astăzi că aplicațiile noilor tehnologii ale informației au un impact semnificativ asupra managementului conflictelor și crizelor și acest impact este de așteptat să crească în viitorul apropiat. Acest articol examinează câteva avantaje și dezavantaje ale dezvoltării acestor tehnologii în ceea ce privește elementele cheie ale managementului conflictelor și crizelor: importanța de a fi cât mai pregatit posibil și anticiparea încercărilor adversarului de a desfășura un atac surpriză.

În ce fel și la ce scară aplicarea, prin intermediul atacurilor sau actelor teroriste, a tehnologiilor moderne ale informației poate duce la degradări ale stării de pregătire? Pe baza rezultatelor studiilor desfășurate în ultimele decenii în cadrul diverselor discipline, va rezulta concluzia că introducerea tehnologiei informației generează atât avantaje, cât și dezavantaje.

În multe privinte, această introducere apare a fi ceva în genul „capului lui Janus": pe de o parte ajută potențialul apărător de a-și spori capacitățile de intelligence, diseminarea pe verticală și pe orizontală de intelligence, în cadrul segmentelor sistemelor C4I și a ciclurilor de luare a deciziilor, poate deveni mai rapidă ca oricând. Pe de altă parte, trebuie să se țină cont de multe dezavantaje și capcane periculoase ce pot apare.

Pe lângă creșterea semnificativă a capacităților apărătorului de a obține, analiza, verifica și disemina diferite tipuri de intelligence despre intenții și tipuri de amenințare, va duce și la

* Academia Militară Regală, Breda, Olanda

creștea cantității de informații irelevante. Mai departe, introducerea tehnologiei informației ar putea conduce la apariția unor erori în ceea ce privește controlul situației și avertizarea.

O privire asupra documentelor despre războiul din Golf din 1991 și războiul din Kosovo din 1999, precum și asupra conferințelor, publicațiilor și filmelor promoționale despre războiul viitorului, sugerează, datorită comentariilor militarilor și oamenilor de știință, că era informațională aduce doar beneficii.

De exemplu, remarci ca „gândiți-vă la ceea ar însemna să aveți la dispoziție posibilități de supraveghere a unui câmp de 200 de mile și să fii în stare să trimiți rachete balistice oriunde pe câmp în doar patru minute - o rachetă care merge precis exact unde vrei" sau „sistemul C3I global va fi arma principală a secolului XXI", indică faptul că apariția progreselor tehnologiei informației în domeniul sistemelor C4I (command, coordination, control, comunication and intelligence) aduce beneficii calității și eficienței operațiunilor viitorului. Trebuie, însă, să se pună întrebarea dacă un asemenea optimism este cu adevărat justificat.

Nu cumva aceste promisiuni pe care - tehnologia informației le face sunt prea bune ca să mai fie și adevărate? Care sunt dezavantajele aduse de aceste promisiuni? Nu este legitim a te întreba care sunt potențialele efecte ale inovațiilor tehnologiei informației? Ce impact vor avea și în ce măsură avantajele vor depăși dezavantajele?

Pentru a căpăta profunzimi noi asupra acestor aspecte, articolul se va focaliza asupra unei arii specifice a războiului, și anume cea a răspunsului la avertizările timpurii și starea de pregătire militară și politică împotriva pericolelor ce apar. Articolul se va concentra asupra întrebării dacă, și în ce măsură, aplicarea tehnologiilor moderne ale informației va avea efecte pozitive și/sau negative pentru starea de pregătire a comandanților militari și liderilor politici în contextul pericolelor prezente și viitoare.

Pentru început, vom prezenta pe scurt esența stării de pregătire politico-militare și a avertizărilor. Va fi discutat apoi impactul

tehnologiilor informației și al războiului informațional asupra câtorva factori cheie prezenți în așa-numitul ciclu de intelligence, cum ar fi detectarea potențialelor pericole, colectarea semnalelor și modelelor de amenințare, interpretarea și diseminarea etc.

După aceasta, va fi pe scurt discutat potențialul impact al noilor tehnologii ale informației asupra reacțiilor de conștientizare, așeptare și evitare din partea liderilor. (vezi și figura 1). Finalul articolului va conține câteva concluzii și recomandări ulterioare pentru studiu.

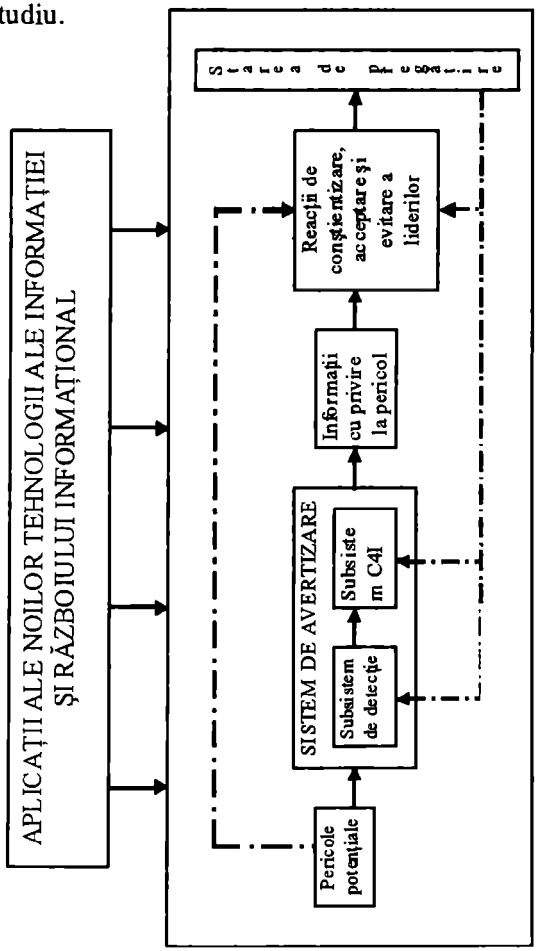

APLICAȚII ALE NOILOR TEHNOLOGII ALE INFORMAȚIEI ȘI RĂZBOIULUI INFORMAȚIONAL
Pericole potențiale
SISTEM DE AVERTIZARE
Subsistem de detecție
Subsiste m C4I
Informații cu privire la pericol
Reacții de conștientizare, acceptare și evitare a liderilor
Starea de pregătire

Figura 1. Modelul conceptual al analizei prezentate

Starea de pregătire poate fi caracterizată ca fiind un concept familiar, dar în același timp normativ, complex și interpretabil. Pentru a înțelege implicațiile dezvoltării continue a tehnologiei informației, este necesar să se înceapă cu o definiție a stării de pregătire. Definiția ce urmează combină elementele aflate în descrierile din dicționare, doctrine militare, studii de război și proceduri.

Măsura în care o entitate (prezentată în acest articol ca un grup mic de persoane politice sau militare aflate în poziții cheie) este pregătită la nivel mental, conceptual, fizic, organizațional și politic pentru a răspunde pe cât de optim este posibil (avându-se în vedere capabilitățile) la diverse pericole din primele faze ale unui conflict.

Starea de pregătire poate fi privită din perspectiva a trei dimensiuni intercorelate:

1. Prima dimensiune include starea și oportunitatea anticipării și vigilenței mentale (a factorilor de decizie cheie), cu privire la materializarea pericolelor anticipate, precum și la efectele imediate și implicațiile pe termen scurt și lung.

Această dimensiune se referă la gradul în care autoritățile politice și militare cheie anticipează la nivel conceptual și mental pericolele. Mai clar, ea cuprinde măsura în care autoritățile politice responsabile au anticipat *mental* o stare de vigilență cu privire la:

(a) probabilitatea unei acțiuni ofensive împotriva lor;

(b) tipul acțiunii;

(c) locațiile unde pericolul (ofensiva adversarului) a acționat;

(d) sincronizarea acțiunilor;

(e) tăria și punctele slabe ale pericolului (de exemplu, trupele inamice in comparație cu punctele forte și slabiciunile apărării);

(f) obiectivele ofensivei și locul acestora în strategia inamicului;

(g) impactul și consecințele imediate.

2. A doua dimensiune esențială este formată din starea și oportunitatea vigilenței unui factor de decizie, precum și gradul de pregătire necesar pentru a utiliza componentele conceptuale,

fizice și mentale ale „măsurilor obișnuite" și „măsurilor de urgență" ce pot fi aplicate imediat când apare un pericol, cu scopul de a minimiza riscurile imediate și pe termen lung, precum și costurile impactului.

3. A treia dimensiune, care poate fi crucială pentru factorii politici de decizie (în special în timpul operațiunilor altele decât războiul), privește gradul în care autoritățile naționale au acumulat suficient suport politic, deoarece acesta este necesar unui răspuns optim în fața pericolului și consecințelor sale.

Această dimensiune se referă la nivelul de anticipare al factorilor de decizie în ceea ce privește contramăsurile de protecție și încercarile de „educare a publicului" pentru a asigura consensul politic care ar putea fi necesar:

(a) pentru a face față (de exemplu a minimiza sau preveni) impactului și/sau implicațiilor unui pericol;

(b) pentru a realiza consensul și sprijinul public și politic care ar putea fi necesar pentru a asigura fezabilitatea și eficiența unor contramăsuri rapide, precum și sprijin pentru implicațiile acestor contramăsuri. Acest lucru include sprijinul, sau cel puțin acceptarea, din partea grupurilor care nu sunt direct implicate în aspectele operaționale militare (presa, publicul, alte departamente, potențialii aliați) pentru posibilele opțiuni de management al crizei.

„Avertizările" pot fi privite ca : *O combinație de indicatori, modele, precum și mesaje scrise care pot fi observate, auzite, citite sau reconstituite de unul sau mai mulți receptori, și prin care aceste date asigură predicții mai mult sau mai puțin incerte și detaliate despre una sau mai multe dimensiuni ale unui potențial pericol și prin care acestea creează un interval de timp suficient pentru a pregăti contramăsuri de protecție.*

Ca și starea de pregătire, avertizările prezintă mai multe dimensiuni. Cele prezentate în cele ce urmează pot fi identificate în cele mai multe cicluri de intelligence și procese de avertizare:

(l) conținutul;

(2) perioada de timp de avertizare;

(3) accesibilitatea;

(4) siguranța;

(5) calitatea;

(6) cantitatea.

Studii despre comunicații publice și organizaționale au indicat că aceste dimensiuni, și în special combinația valorilor specifice ale acestor dimensiuni, pot afecta în mod semnificativ gradul de conștientizare al liderilor, precum și deschiderea pentru acceptare și reacție la semnalele de avertizare.

După definirea stării de pregătire și avertizări, este acum timpul să se discute despre potențialul impact pe care aplicarea noilor tehnologii ale informației îl are asupra:

(l) procesului de detectare a potențialelor pericole;

(2) colectării, diseminării și interpretării potențialelor semnale de avertizare;

(3) conștientizării, interpretării, reacțiilor de acceptare sau respingere a liderilor politici și militari;

(4) stării de pregătire pentru confruntarea cu pericolele actuale și viitoare.

Pentru agenții de intelligence ca Agenția națională de securitate (NSA - National Security Agency) și CIA - Central Intelligence Agency, impactul noilor tehnologii ale informației asupra semnalelor de avertizare și indicatorilor de amenințare este în creștere. Sistemele de avertizare timpurie, posibilitățile de interceptare și ascultare, precum și posibilități tehnologice de colectare vizuală devin tot mai răspândite și sofisticate.

Experiențe, ca războiul din Golf, testele nucleare ale Pakistanului în timpul crizei cu India din mai 1998, campania aeriană din Kosovo și unele mișcări surpriză ale lui Miloșevici și ale armatei sale au subliniat necesitatea de a nu supraestima puterea oferită de tehnologia informației. Multe obiecte statice și în special cele mobile sunt încă dificil de urmărit cu precizie, în special când trebuie identificate de la înălțime, în scurt timp și în condiții

meteo proaste. Machetele se pot utiliza încă cu succes pentru a induce în eroare.

Ultimul deceniu (și în special ultimii ani) sugerează că, în comparație cu posibilitățile de a colecta avertizările, cea mai mare inovație în domeniul „stării de pregătire și atacurilor prin surprindere" pare a fi în ceea ce privește diseminarea de intelligence, aspectele legate de sistemele C4I și ciclurile de luare a deciziilor. În principiu, potențialii atacatori și apărători pot profita în multe feluri de acestea. Nu ar fi însă înțelept să se neglijeze sau minimalizeze influențele negative ce pot apare.

De exemplu, nevoia în creștere pentru a avea date în timp real poate crește gradul de conștientizare al comandantului asupra situației, dar în același timp crește șansa ca motivația analiștilor și experților de intelligence pentru verificări, analize și interpretare a datelor să scadă.

Mai mult ca oricând, analiștii vor trebui să se confrunte cu dilema dacă sau nu ar trebui să disemineze date și să consilieze superiorii mai rapid, dacă vor să aibă influență asupra factorilor de decizie și să devină o sursa de încredere a comandantului (dar cu riscul de a-și pierde credibilitatea în cazul unei evaluări greșite).

Experiențele trecute și recente arată că introducerea noilor tehnologii ale informației tinde să aibă un mare impact asupra celor mai multe dimensiuni ale semnalelor de avertizare, impact în multe privințe încă imposibil de controlat. În continuare este aruncată o privire mai atentă asupra impactului probabil asupra diverselor dimensiuni ale avertizării.

Dimensiunea 1: Conținutul

Avertizările cuprind elemente de informație cu privire la unul sau mai multe aspecte ale conținutului unui pericol iminent:

1. estimare a probabilității ca pericolul (atacul) să se materializeze ***(dacă)***;

2. determinarea identității precise a atacatorului ***(cine)***;

3. determinarea tipului acțiunilor și tehnologiilor implicate ***(cum)***;

4. identificarea locației care va fi în pericol (atacată) ***(unde)***;

5. predicția momentului de timp la care pericolul se poate materializa ***(când)***;

6. evaluarea motivelor și obiectivelor ce stau la baza pericolului ***(de ce)***.

La prima vedere pare evident că introducerea tehnologiilor moderne ale informației va face ca îmbunătățirea calității avertizării în raport cu fiecare din aceste aspecte să se facă mai ușor. Apărătorii vor dispune de semnale, modele și evaluări ale avertizărilor și amenințărilor mai detaliate, sigure și mai bine controlabile decât oricând înainte.

În același timp, însă, apar multe dezavantaje și capcane. O capcană relativ nouă, care este acum mai relevantă ca oricând, este *sindromul WYSIWYG* (what you see is what you get). Liderii și analiștii care au la dispoziție date în timp real și adesea vizualizate și care pot oferi informații despre una din dimensiunile arătate mai sus, vor avea adesea dificultăți în a rămâne prudenți în ceea ce privește posibilitatea de a se înșela singuri și/sau de a fi înșelați de adversari. Impactul informațiilor vizuale asupra minții umane poate conduce la percepții greșite și eșecuri. De exemplu, există întotdeauna șansa ca atacatorul să-și schimbe planurile în ultimul moment în timp ce apărătorul încă gândește și acționează pe baza ultimelor imagini pe care le are.

Chiar mai mult, situația actuală a pericolelor iminente poate să se schimbe, semnificativ datorită dinamicii situației și momentului de timp între trimiterea și primirea semnalelor. Deși liderii pot fi conștienți de aceasta, pot fi în schimb supuși mai mult ca oricând unor presiuni interioare pentru a lua decizii rapide. Faptul că acești lideri sunt pe deplin conștienți că alții văd aceleași „imagini în timp real" și ar putea să se întrebe de ce nu se ia nici o decizie (de vină poate să fie același sindrom) poate deveni o sursă de presiune.

În plus, doctrinele și instrucția pot fi cruciale pentru a face trecerea la cicluri decizionale mai rapide decât ale adversarului, așa cum impactul presei (de exemplu, efecte de tip CRM și Internet) poate deveni o sursă majoră de termene limită autoimpuse.

Dezvoltările tehnologice pot crește probabilitatea ca liderii și analiștii să cadă în alt tip de capcană cognitivă și psihologică. Aceasta este reprezentată de faptul că oamenii pot deveni obsedați de date vizualizate în timp real, acordând o foarte mare parte din timp pentru aceasta. Prețul ar putea fi că ei aproape trec cu vederea elemente complexe și cruciale de intelligence (care sunt însă mai puțin accesibile și controlabile) care ar putea oferi introspecții interesante despre unul sau mai multe aspecte ale conținutului pericolului iminent.

Dimensiunea 2: Intervalul de timp

Altă dimensiune crucială a avertizărilor este așa-numitul *interval de timp* între momentul avertizării și momentul care este previzionat pentru materializarea pericolului. Această dimensiune este adeseori denumită și „interval de avertizare". La modul ideal (din perspectiva apărătorului), avertizările detaliate și sigure sunt acelea care se produc la un moment de timp la care este posibilă luarea unor măsuri adecvate de protecție.

Istoria arată că introducerea diverselor tehnologii în ultimele secole are un imens impact asupra intervalului de avertizare. Probabil cea mai revoluționară schimbare în război și managementul crizelor a fost creșterea exponențială a gradului de mobilitate. Această creștere comprimă timpul și spațiul, sporește mobilitatea trupelor, capabilitățile ofensive și defensive.

Pe măsură ce mobilitatea crește, intervalul de timp pentru contramăsuri scade semnificativ, de la luni sau săptămâni în secolul XIX, la săptămâni sau chiar zile în epoca căilor ferate, tancurilor și motoarelor cu combustie, la zile sau ore în era aviației și la ore sau chiar minute în era nucleară (vezi figura 2).

Tendința care s-a manifestat în trecut pare a se manifesta astăzi cu și mai mare intensitate. Utilizarea ultimelor noutăți tehnologice de către unul sau mai mulți adversari poate reduce mărimea intervalului de avertizare spre zero. Cum atacurile informaționale și operațiunile psihologice pot să se desfășoare în tăcere, va fi din ce în ce mai complicat și câteodată chiar imposibil să se repereze începutul unui atac informațional sau să se determine cine, cum, și de ce îl desfășoară.

Ar putea deveni chiar greu de determinat cât timp pot fi întârziate evaluarea amenințărilor, luarea deciziilor și implementarea contramăsurilor până când întreaga infrastructură C4I a apărătorului să fie serios afectată și un răspuns adecvat să nu mai fie posibil. Rolul crescând al războiului informațional ridică rapid bariera clasică dintre război și pace.

Ca o consecință, recentele progrese tehnologice pot pune la îndoială procesele de evaluare și nivelul de conștientizare ale apărătorului în ceea ce privește probabilitatea, momentul de timp, locul, inițiatorul și impactul unui atac, precum și strategia și tacticile atacatorului. În fapt, tipuri de arme ce rămân neobservate și computere „silențioase" există de câțiva ani încoace și vor exista cu siguranță și în continuare.

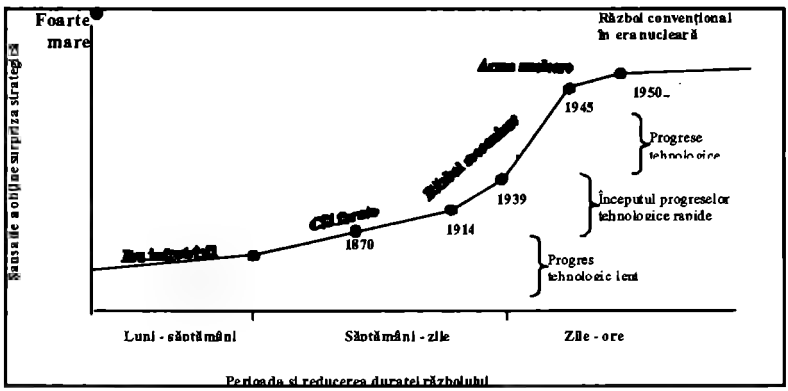


Figura 2. Model conceptual al reducerii duratei războiului datorită inovațiilor tehnologice și impactul asupra șanselor de a obține surpriza strategică

Dimensiunea 3 : Accesibilitatea

Una din problemele structurale cele mai mari în legătură cu avertizările care a apărut evidentă în timpul atacurilor surpriză și confruntărilor cu dezastrele naturale nu este faptul că nu a existat intelligence adecvat la timp, ci faptul că, comandanții și autoritățile au fost în mod frecvent informați neadecvat de către subordonați sau colegi în legătură cu intelligence-ul care a fost colectat și produs.

Lipsa de accesibilitate poate fi cauzată de mai mulți factori. De exemplu, compartimentarea și prea multă secretomanie, prea multă specializare și fragmentare, teama de a pierde credibilitatea în cazul unei alarme false, sindromul „intelligence la comandă", proceduri prea lungi și complexe etc. Rămâne de văzut dacă beneficiile introducerii noilor tehnologii vor putea depăși dezavantajele. Într-adevăr, cel puțin teoretic, liderii militari și politici vor avea mai multe oportunități de a beneficia de intelligence și de a scurtcircuita hățișurile ierarhice din sistemele C4I.

În același timp, se poate cu ușurință ajunge la tipuri greșite de date, supraîncărcare cu informații și un sentiment fals de control. Mai mult chiar, se poate ajunge la reacții greșite în cazul lucrului cu informații brute ale căror detalii subtile sunt trecute cu vederea sau prost percepute și se poate ajunge la ignorarea unor semnale și indicatori care sunt mai puțin accesibili, dar care pot fi la fel de importanți în luarea unor decizii corespunzătoare (de exemplu date cu privire la motivațiile adversarului, strategii și planuri ascunse).

Dimensiunea 4: Gradul de încredere

Multe din studiile despre răspunsurile la avertizări și starea de pregătire indică faptul că gradul de încredere al sursei de la care cineva primește semnale și avertizări are o influență semnificativă asupra deciziei dacă trebuie, sau nu, să se acționeze în urma avertizării. Cu cât este mai mare gradul de încredere al

unei surse în ochii beneficiarului, cu atât este mai probabil ca informația trimisă să fie acceptată fără o evaluare critică și se va acționa pe baza ei. Dacă o sursă nu este considerată de încredere, informațiile provenite de la ea vor fi mai degrabă evitate sau ignorate. Datorită impactului Internetului și CRM-ului, ca surse dominante de informații în permanentă actualizate, distincția dintre cele două tipuri de surse de informații amintite mai sus devine greu de realizat. Este un paradox faptul că agențiile de intelligence care frecvent încearcă să afecteze pe alții prin manipularea informațiilor diseminate prin Internet și agențiile de știri pot deveni victime ale acelorași mijloace mass-media. Convingerea că ești capabil de a distinge între informații sigure și informații nesigure se poate dovedi o capcană care poate afecta întregul proces de intelligence, cât și gradul de credibilitate al acestor agenții.

Dimensiunea 5 : Calitatea

Una din cele mai importante dimensiuni a avertizărilor este calitatea, cu alte cuvinte gradul în care o avertizare prezintă certitudine, acuratețe și predicții detaliate. Este important de observat că cei mai mulți factori de decizie trebuie, conștient sau inconștient, să realizeze o evaluare a avertizărilor despre care sunt preveniți că nu sunt chiar așa de încredere și precise în loc de a face o evaluare post-factum a avertizărilor care s-au dovedit a fi mai puțin precise.

Dimensiunea 6: Cantitatea

Cantitatea avertizărilor primite (adică numărul de semnale de avertizare primite de agențiile de intelligence și factorii de decizie într-un anume interval de timp în raport cu capacitățile lor limitate de a le procesa corespunzător) este una dintre cele mai menționate dimensiuni ale avertizărilor. La fel ca alte dimensiuni, modul în care cantitatea este folosită depinde de ce semnale, mesaje sau modele sunt denumite avertizări.

Evenimente recente (genocidul din Ruanda din 1994, atacul irakian asupra Kuweit-ului din 1990 sau criza din Kosovo din 1998-1999) arată că este probabilă o creștere spectaculoasă a cantității de indicatori asupra potențialelor amenințări. Aceleași evenimente ilustrează că tehnologiile sofisticate (sateliți, capabilități de interceptie etc.) împreună cu iluzia creată că a dispune de capacități mai bune și mai rapide de colectare reprezintă o garanție a succesului, tind să ducă la creșterea „apetitului" organizațiilor și factorilor de decizie pentru mai multe date în timp real. Totodată, însă, există șansa ca suprasaturarea cu informații a analiștilor, politicienilor și militarilor să crească.

Facilități mai performante vor duce adeseori la creșterea nevoilor comandanților și autoritaților pentru intelligence detaliat, rapid și actualizat cu scopul de a crește gradul de cunoaștere a situației. În același timp, și poate că la prima vedere pare paradoxal, este probabil că aceștia vor „trăi" perioade în care se vor simți „subîncărcați" cu informație. Se poate distinge aici un model comportamental care este prezent și în multe alte domenii. Cu cât bunăstarea este mai mare, cu atât așteptările sunt mai mari, ambițiile vor fi mai înalte și frustările în caz de neîmplinire vor fi mai mari.

Studii efectuate asupra atacurilor prin surprindere în ultimele patru decenii au arătat că cele mai multe avertizări conțin multe semnale distorsionate, precum și diferite grade de incertitudine și ambiguitate în ceea ce privește toate dimensiunile avertizărilor și pericolelor iminente.

Unul dintre cei mai importanți factori implicați în eșecuri în privința intelligence și atacurile surpriză este ceea ce se numește sindromul „cry wolf". Cu cât mai multe avertizări și alerte sunt considerate false (din diverse motive, cum ar fi acela că atacatorul și-a schimbat intențiile sau că agențiile de intelligence au fost insuficient informate despre momentul și locul apariției pericolului), cu atât este mai probabil ca credibilitatea avertizărilor ulterioare să scadă și procesul de „desensibilizare" la avertizări

să devenină dominant, efectul fiind, bineînțeles, interpretări și răspunsuri greșite la avertizări viitoare relevante.

De exemplu, în timpul războiului din Coreea, stafful generalului MacArthur, sursa principală de intelligence, a avertizat, pe perioada câtorva luni, Washington-ul despre iminența unui atac nord-coreean. Când acel atac a avut loc, secretarul apărării Louis Johnson l-a considerat ca fiind doar o altă violare a frontierei.

Toate aceste avertizări au fost la urma urmei precise deoarece cele două state coreene erau angajate într-o bătălie de artilerie prelungită însoțită de dese treceri ale frontierei. Concluzia care se desprinde este că dacă cineva striga „Lupul! Lupul!" de prea multe ori, s-ar putea ca atunci când într-adevăr apare lupul, să nu-l bage nimeni în seamă.

Este de așteptat deci ca introducerea noilor tehnologii ale informației nu doar să ducă la creșterea calității procesării avertizărilor, ci și să conducă la diverse forme de informații irelevante („zgomot") și sindromuri gen „cry wolf".

Inducerea în eroare a fost întotdeauna un element principal al desfășurarii războiului. Se înțelege prin inducere în eroare mascarea intențiilor reale ale cuiva, a capabilităților, manevrelor și concentrărilor de forțe cu scopul de a obține un atac surpriză sau o mișcare defensivă surpriză. Inducerea în eroare este realizată în mai multe moduri:

- răspândirea de zvonuri false ;
- mascarea funcționării legăturilor radio, aranjarea unor rețele radio false, radio-inducere în eroare;
- introducerea unor informații false în sistemele de securitate, rețelele de date sau Internet;
- dispunerea unor machete;
- ascunderea obiectelor reale și a manevrelor pentru a împiedica recunoașterea și observarea;
- schimbarea aspectului exterior al obiectelor și manevrelor;
- producerea de „zgomot" artificial;
- utilizarea virușilor de computer și războiului electronic.

Așa cum războaiele și bătăliile recente au demonstrat, tehnologiile informației vor juca un rol semnificativ în fiecare din aceste forme de inducere în eroare. Operațiile informaționale de inducere în eroare pot determina apărătorii, dar și potențialii atacatori, să facă judecăți și să ia decizii greșite.

Datorită introducerii noilor tehnologii ale informației în acțiunile de inducere în eroare, oricând ar putea deveni mai ușor pentru un agresor sofisticat să „îndeplinească" așteptările apărătorului de o manieră bine coordonată, furnizându-i acestuia „ponturi" subtile și la prima vedere cu un grad de încredere ridicat. Este, de asemenea, mai ușor, cu ajutorul tehnologiei informației, să se pătrundă în ciclurile de luare a deciziilor ale adversarului.

Chiar mai mult, datorită inovațiilor în domeniul sistemelor de interceptare, poate deveni mai ușor să se verifice dacă, și eventual în ce măsură, strategiile și tacticile de inducere în eroare reușesc.

Studiile din ultimele decenii în domeniul științelor comunicării, științelor cunoașterii și managementului au subliniat în mod constant că o creștere exponențială a tehnologiilor de producere a informației a mărit discrepanța dintre producerea de informație și capacitățile umane de a utiliza această informație. Cu alte cuvinte, producerea și colectarea mai multor informații nu înseamnă strict mai multe informații, iar mai multe informații nu înseamnă siguranță, același lucru cu utilizarea informației.

În timp ce tehnologiile de producere și diseminare a mai multor informații și într-un mod mai rapid au crescut aproape exponențial, capacitățile umane de a filtra și procesa aceste date nu cresc în aceeași măsură. Cu alte cuvinte, chiar dacă liderii vor vrea și vor putea să dispună de mai mult timp pentru procesarea avertizărilor primite, este încă foarte probabil ca multe semnale relevante să fie ignorate. Distanța între ceea ce analiștii de intelligence și liderii politico-militari știu și ceea ce aceștia ar putea ști (având în vedere datele pe care le-au avut și le au la dispoziție) devine din ce în ce mai mare.

Uneori semnalele vor trece neobservate ca o consecință a unor decizii deliberate de a concentra resursele (care sunt puține) pe interpretarea unui tip de surse și de a ignora datele din alte surse. Rezultatul este acela că factorii politici vor fi frecvent confruntați cu mari discrepanțe între datele puse la dispozitie, informațiile pe care le cer, informațiile de care au cu adevărat nevoie și datele pe care de fapt le procesează și utilizează (figura 3).

În această figură, semnificația notațiilor este următoarea:

1. toate informațiile pe care le are factorul de decizie;
2. informațiile pe care factorul de decizie vrea să le aibă;
3. informațiile pe care factorul de decizie are nevoie să le aibă;
4. toate informațiile despre un anume conflict;
5. semnalele de avertizare despre un conflict anume;
6. informațiile pe care factorul de decizie le primește ca rezultat a strategiilor sale.

Dreptunghiurile nu sunt la scară și în realitate ele sunt într-o evoluție dinamică, depinzând de mediul social al factorului de decizie, de problema în sine etc.

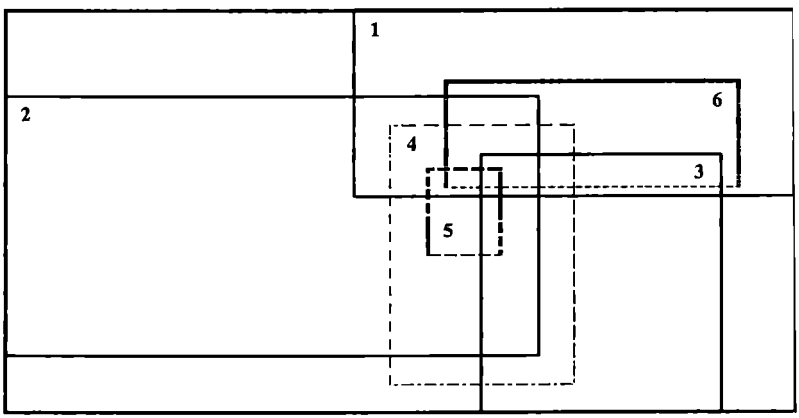


Figura 3. Relațiile conceptuale dintre diversele forme de informații cu care este confruntat un factor de decizie

Pregătirea, educarea și exercițiile

Numeroase amenințări, precum și misiuni de tip tactic au nevoie de un înalt nivel de pregătire. Scopul tuturor măsurilor trebuie să fie obținerea:

• Dorința individuală și abilitatea de a accepta responsabilitatea;

• Abilitatea de a delega;

• Generarea unui înalt grad de sensibilitate în ce privește capacitățile potențiale de operații informaționale ale adversarului;

• Dorința de a obține capacități adecvate de utilizare tehnică a echipamentului de folosire a tehnologiei informaționale și de comunicare;

• Educația și antrenarea stabilității psihologice a individului pentru a contracara doctrinele și procedurile adversarului.

Aceasta din urmă merită un interes particular în cazul măsurilor de menținere a păcii și/sau de impunere a păcii în cadrul misiunilor Națiunilor Unite.

Beneficiile unei coaliții constau în combinarea capacităților operațiilor informaționale a diferiților parteneri, ceea ce furnizează o mai largă varietate de opțiuni și instrumente în mâna comandanților militari. Dar pe de altă parte, noi vulnerabilități pot apărea, iar vulnerabilitățile existente se pot multiplica în cadrul coaliției.

Chiar dacă fiecare parte s-a adaptat cu succes la provocările operațiilor informaționale, fricțiuni există încă (sau altele noi pot apărea). Aceste fricțiuni care sunt inerente unei coaliții, provin din surse diferite:

• **Aspecte umane**: Pot exista tensiuni între națiunile participante, ce-și au originea în probleme istorice, culturale, religioase sau etnice, de limbaj.

• **Aspecte tehnice**: Interconexiuni ale diferitelor sisteme de tehnologie informațională și de comunicare pot duce la posibile puncte slabe.

• **Aspecte organizaționale**: Structuri diferite de forțe, structuri de C2 sau principii de conducere pot prejudicia operațiile informaționale în cadrul unei coaliții.

Un oponent va încerca să identifice și să exploateze aceste puncte slabe.

Operațiile informaționale defensive

Pentru a contracara aceste vulnerabilități și amenințări, pentru a veni în întâmpinarea dezvoltărilor viitoare, capacitățile de operații informaționale trebuie să fie dobândite. Acest lucru presupune supraviețuirea pe scară largă a sistemului.

Una dintre cerințele majore ale unei asigurări informaționale adecvate este stabilirea unei infrastructuri informaționale și de comunicare, de urgență, care să fie valabilă 24 de ore din 24 și 7 zile pe săptămână.

Asigurarea informațională va deveni o „stare naturală" în cadrul forțelor armate. Pentru a menține asigurarea informațională a unei națiuni sau a unei coaliții multinaționale, este necesară o recunoaștere precisă a amenințărilor operațiilor informaționale asimetrice.

Eforturile adversarului de recunoaștere a operațiilor informaționale trebuie detectate, analizate și înțelese. Acest lucru cere o cunoaștere combinată de intelligence și de operații informaționale. De aceea asigurarea informațională trebuie să fie considerată ca fiind un interes comun al tuturor țărilor NATO.

Capacități active de operații informaționale ofensive ar trebui dezvoltate în cazul Olandei și Germaniei. Atunci când te decizi să dezvolți astfel de capacități, spectrul capacităților operațiilor informaționale dobândite de ceilalți parteneri NATO trebuie luat în calcul. În plus, restricțiile legale existente trebuie examinate în scopul de a câștiga o fundamentare juridică solidă pentru folosirea efectivă a operațiilor informaționale.

Documentele de politică a operațiilor informaționale defensive și ofensive trebuie publicate pentru a ajuta la clarificarea termenilor, definițiilor și responsabilităților. O doctrină comună a operațiilor informaționale ar trebui publicată și permanent actualizată. Toate categoriile de forțe ar trebui să-și implementeze această doctrină.

Folosirea unor astfel de sisteme și interoperabilitatea ar trebui să fie conduse de necesitatea operațională, de asigurarea informațională, supraviețuire, flexibilitate, disponibilitate, performanță, costuri și riscuri reziduale.

Deoarece operațiile informaționale ar trebui să fie parte integrantă a tuturor operațiilor militare combinate, este nevoie de planificare și coordonare printre elementele cartierelor generale integrate, a conducerii și a altor agenții.

Un element organizațional capabil să combine toate aceste activități și să dezvolte orientare și planificare pentru operațiile informaționale poate fi o celulă de operații informaționale (IOC), formată din reprezentanți din fiecare conducere, componente și agenții de sprijin responsabile pentru integrarea capacităților și activităților. Figura 2 ilustrează o privire de ansamblu a unei posibile celule de operații informaționale.

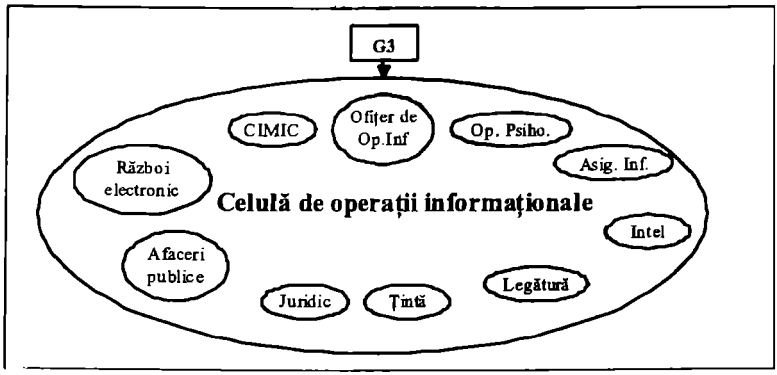


Figura 2: Compoziția unei celule de operații informaționale

Ministerele de apărare au ocazia să joace un rol important în procesul în creștere a nevoii de asigurare informațională a altor autorități publice și guvernamentale. Cunoașterea asupra operațiilor informaționale defensive trebuie împărțită între forțele armate, organizațiile de apărare civilă, structurile de comandă și ramurile de industrie critice (energie, transport, comunicare, etc.)

Riscurile fluxurilor informaționale în cadrul coaliților trebuie bine înțelesă și de câte ori este posibil, redusă. Componenta de apărare a MEII trebuie privită ca element de sprijin pentru autoritățile civile și pentru funcțiile economice critice, atât în interesul națiunii cât și în sprijinul NATO și UE.

Acțiuni recomandabile

Grupul de studiu a propus următoarea listă de acțiuni:

- Stabilirea unei capacități centralizate și controlate de asigurare informațională;
- Exploatarea cunoașterii prezente a operațiilor informaționale;
- Crearea unei structuri de rezervă, de personal, care posedă cunoștințe și experiență în domeniul operațiilor informaționale sau care provine din medii etnice, religioase și culturale (PSYOPS, CIMIC);
- Dezvoltarea și menținerea unei politici naționale de operații informaționale (care să se bazeze pe MC 422 a NATO) și o doctrină integrată de operații informaționale;
- Implementarea simultană a politicii comune de operații informaționale de către toate categoriile de forță;
- Cercetarea națională și internațională permanentă în zona de operații informaționale, asigurare informațională și protecție de infrastructură critică;
- Definirea la nivel național a capacităților dorite de operații informaționale ofensive, luând în calcul și alte capacități ale națiunilor membre NATO;
- Definirea și armonizarea legilor naționale și internaționale;
- Stabilirea de celule de operații informaționale la nivele integrate și combinate;
- Definirea unui minim esențial de infrastructură informațională națională, binațională și multinațională;

Implementarea de grupuri de lucru interagențiale care să includă toate sectoarele relevante ale societății.

RĂZBOIUL INFORMAȚIONAL PROBLEME și PERSPECTIVE

VASILE PĂUN

Așa cum am mai afirmat, R.I. este adesea înțeles ca război al epocii informaționale. Această înțelegere a R.I. se sprijină pe o idee destul de răspândită potrivit căreia societățile informaționale succed societăților industriale"[44]. Într-adevăr, numerizarea, dezvoltarea capacităților de stocare a datelor, multiplicarea sateliților de comunicații creează condițiile unui mediu foarte diferit de cel cunoscut până în prezent: relațiile interumane se modifică, apar noi ritmuri.

Cum ar putea ca teoria și practica războiului să nu fie afectate de aceste schimbări? Ce presupune efectiv un R.I.? Este vorba de o modă pasageră care solicită spiritul imaginativ al analiștilor sau este „principala caracteristică a conflictului secolului al XXI-lea"[45]? Cum abordează statele o astfel de provocare? Ce semnificație trebuie atribuită în era informațională termenilor utilizați în Carta O.N.U.: „forță", „atac armat", „agresiune armată"?

Acestea nu sunt decât doar câteva dintre întrebările care apar natural când se vorbește despre R.I. și care merită o tratare mai atentă.

---

[44] Alvin Toffler, Război și anti-război, Ed.Antet, 1995.

[45] Christian Malis, „Renseignement el information, *l'Armement*", dec. 1997-ian. 1998.

EXCURS IN SPAȚIUL CONCEPTELOR

Provocarea nu este de a impune o nouă idee în gândirea militară, ci de a o elimina pe cea veche.

Basil Liddell-Hart

A devenit o obișnuință să se vorbească și să se declare intrarea într-o epocă a informației. „Moda" a venit dinspre Statele Unite unde s-au succedat pe rând mai multe noțiuni cum ar fi cele de „economie informațională" sau „război informațional". Din perspectiva soților Toffler, anumite state părăsesc societatea de tip industrial pentru a aborda un nou teritoriu, cel al „societății celui de-al treilea val", în care teritoriul, populația și resursele naturale devin mai puțin importante decât capitalul uman, iar faptul de a poseda informația potrivită conduce la o modificare sensibilă a activității economice, a formelor sociale, a modurilor de conflict.

O expresie des utilizată în mediul militar, în special, este cea a „R.I.". Sensul exact al termenului nu a fost încă unanim stabilit și acceptat, mai ales din cauza faptului că acesta descrie un ansamblu de probleme care par să nu aibă nimic în comun. Ambiguitatea termenului crește pe măsură ce sunt utilizate expresii ca „război în ciberspațiu", „razboi în rețea", „războiul celui de-al treilea val", „război post-industrial"[46].

Pentru majoritatea analiștilor militari, R.I. reprezintă o utilizare în scopuri militare a calculatoarelor și a altor tehnologii împotriva unui stat, ca alternativă la atacurile convenționale. Acesta include activități care nu corespund, în mod normal normelor militare, dar care reflectă creșterea dependenței activităților guvemamentale și comerciale de diverse sisteme, vitale pentru buna funcționare a operațiilor militare moderne.

[46] John Arquilla și David Ronfeldt, *Cyberwar in Coming*, RAND, 1992

Pentru alți analiști este vorba de o idee mai largă care juxtapune impactul erei informaționale cu dezvoltarea diverselor tipuri de conflicte sociale și politice având ca efect erodarea statului-națiune și a „monopolului său asupra violenței organizate".

O comparație cu efectele politice ale primei revoluții a informației a Europei moderne poate fi utilă. Inventarea modului de distribuție a cărților a favorizat, după anul 1500, transformarea conștiinței europene. Această transformare a privilegiat, între altele, apariția statelor-națiune, asigurând în același timp conducătorilor posibilitățile de a mobiliza loialități naționale și de a dezvolta administrații centralizate. Pe termen lung, cele care nu au avut nimic de câștigat au fost entitățile supranaționale și cele subnaționale (ca instituția Papalității și autoritățile feudale) care nu au știut să profite de noul mediu.

Actuala revoluție informațională ar putea avea un efect invers, căci globalizarea și personalizarea sistemului de comunicare electronică par să submineze autoritatea statală și să ușureze trecerea puterii spre mișcările subnaționale și spre cele transnaționale, mai ales a celor care ating sensibilități etnice, religioase sau culturale.

Secolul al XX-lea este caracterizat de îmbinarea dintre știință și tehnică (rebotezată cu numele mai nobil de tehnologie). Evident că și anterior s-au înregistrat progrese remarcabile în cunoașterea științifică și în realizările tehnice și s-au stabilit legături între teorie și practică, între domeniul cunoașterii „pure" și cel al „aplicațiilor", însă, până în secolul nostru, știința și tehnologia au evoluat mai mult sau mai puțin în paralel, sprijinindu-se mutual, având însă raporturi cotidiene mai degrabă slabe, în a doua parte a secolului al XX-lea (de la al doilea război mondial) electronica a invadat lumea, găsind-o de acum pretutindeni: acasă, la locul de muncă, în mașini etc. Calculatorul a abolit, în final, deosebirea dintre științele „pure" sau „fundamentale" și cele „aplicate", împingând din ce în ce

mai departe barierele care, până atunci, izolaseră prelucrarea informației. Știința este de acum omniprezentă în viața materială, iar inovațiile se succed într-un ritm accelerat. Universitățile nu mai au monopolul cunoașterii. Ele trebuie să se asocieze cu întreprinderile pentru cercetare și pentru educație. Cercetarea, altădată luxul țărilor bogate, a devenit un factor de producție. Munca umană își schimbă deja natura. Cuplul, de acum de neseparat, al științei și tehnologiei transformă condițiile prosperității și ale puterii.

Adevărata mutație, caracteristică celei de-a doua jumătăți a secolului al XX-lea, este cea a tehnologiilor informaționale. Energia și informația, de exemplu, întrețin legături profunde. A obține o informație e ca și cum ai câștiga energie de calitate superioară, în orice domeniu, a dispune de informație înseamnă a merge mai sigur și mai direct spre scop și, în consecință, a economisi energie.

În ciuda schimbărilor deja înregistrate, fără îndoială, nu facem decât să întrevedem consecințele acestei revoluții informaționale. Relațiile internaționale sunt deja profund afectate de impactul tehnologiilor informaționale. În prezent, statele controlează piețele financiare mai puțin decât supraveghează piețele financiare statele. Astăzi „efectul CNN", mâine, fără îndoială, „efectul Internet" este cel ce va invada spațiul politic.

Este pusă în discuție problema guvernării societăților, pentru că statele sunt prinse în clește între influențele externe, din ce în ce mai constrângătoare, și creșterea marjelor interne de autonomie (întreprinderi, asociații, colectivități locale sau regionale etc).

În domeniul militar, armele devin mai precise, mai eficiente și se diversifică, dar cursa dintre spadă și scut continuă, știința putând să servească *a priori* și unuia și celuilalt. De aceea, nu este deloc surprinzător faptul că aceste schimbări influențează și operațiile militare.

RĂZBOIUL INFORMAȚIONAL. ABORDARE TEORETICĂ

Deși R.I. a fost intuit și conceptualizat încă din 1976 de către Thomas P. Rona [47], conștientizarea posibilității existenței unui altfel de război, al unui război invizibil, mult mai subtil decât războiul clasic, nu s-a realizat decât foarte recent, tonul dându-l mediile militare.

Una dintre primele pietre de construcție ale conceptului de R.I. a constituit-o cartea lui A. Toffler, „Al treilea val", apărută în 1980 [48]". În aceasta se poate citi că „pentru a ataca o națiune se poate obstrucționa fluxul informațiilor - tăierea legăturii dintre sediul societății multinaționale și filialele sale din străinătate, ridicarea de bariere informaționale în jurul ei etc. Vocabularul internațional s-a îmbogățit cu o nouă expresie: „suveranitatea informației".

Această reflecție asupra epocii informaționale a fost continuată de o altă carte a aceluiași autor, intitulată „Război și anti-razboi [49]", care a permis relansarea dezbaterii în Statele Unite asupra conceptului de R.I. Departamentul american al Apărării, care a urmărit aceste reflecții și pe care, în mare măsură, le-a și provocat, a trecut prin mai multe etape, de la conceptul de *Manoeuver Warfare,* aplicabil unui război convențional, la *Strategic Information Warfare.* Acesta este un concept global care acoperă, în același timp, noțiunea de *Conventional Warfare,* care vizează în principal infrastructurile economice ale statului oponent, noțiunea de *Command & Control Warfare,* care privește în mod clasic distrugerea sau neutralizarea forțelor militare adverse și noțiunea *Information Warfare.*

Expresia „R.I." acoperă o serie întreagă de semnificații. Lipsa unei definiții clare a R.I este vizibilă în toată literatura

[47] Thomas Rona (1922-1997) a creat termenul de „război informațional" și a impulsionat cercetările în domeniu.

[48] Publicată și în limba română în 1983, la Editura Politică.

[49] Publicată și de Editura Antet, în 1995.

de specialitate. Până în prezent s-a încercat definirea originilor acestui tip de război, însă nimeni nu i-a stabilit încă principiile. Aproape fiecare persoană care scrie despre R.I se confruntă cu această dificultate. S-au formulat, bineînțeles, mai multe definiții care seamănă între ele. Dar faptul că aproape oricine scrie despre R.I, se simte obligat să-l definească, subliniază această lipsă a unei definiții universal acceptate.

Teoria și practica R.I. se bucură, în ultimul timp, de o atenție crescândă din partea politicienilor, strategilor, oamenilor de știință și mijloacelor de informare în masă din diverse țări, îndeosebi din spațiul nord-atlantic și cel european, fenomen ușor de constatat urmărind frecvența discursurilor publice, conferințelor, simpozioanelor, cărților, studiilor și articolelor care abordează această problemă.

Caracteristica de subiect „fierbinte" este de asemenea pusă în evidență de diversitatea și exotismul unor concepte („infrastructură informațională critică", „operații informaționale"), specializări universitare (strategie cibernetică), instituții (Colegiul de Management al Resurselor Informaționale), preocupări („hacker", „cracker"), toate asociate domeniului R.I.

Deși nu există o definiție universal acceptată, se poate vorbi despre RI. ca fiind o formă nouă de război, dacă sunt avute în vedere instrumentele pe care le utilizează pentru a-și atinge scopurile (grație în special exploziei tehnologiei informaționale). Este însă important de notat că tehnologia informației nu permite doar desfășurarea războiului modern, ci adaugă o nouă dimensiune conflictelor. Infrastructura informațională, prin conținutul său și tehnologiile care o compun, este considerată acum obiect al unui război informațional, dar și subiect de aceeași complexitate strategică cu dimensiunile tradiționale (aeriană, terestră, marină și spațială).

Rețelele informaționale compun un nou câmp de luptă, iar informația însăși devine o țintă. Fiecare a devenit, separat, dar și în combinație cu celelalte, atât armă cât și țintă.

În același timp, se poate vorbi despre R.I. ca fiind o formă veche de război, dacă se face referire la conceptele pe care le are la bază (filosoful chinez Sun Tzu vorbea acum 25 de secole despre „viclenie", despre arta de a înșela adversarul, despre necesitatea de a împiedica adversarul să evalueze corect o anumită situație. Intr-un mod asemănător se exprima și Machiavelli, în secolul al XV-lea, când descria în „Prințul" sau în „Arta războiului" calitățile omului de stat, ale Prințului, care, înainte de toate, este un conducător militar ce trebuie să aibă o natură egoistă, calculată, șireată etc.).

După cum am menționat deja, R.I. nu constituie o practică nouă, din punct de vedere al conceptelor după care se ghidează. Aspecte care ar putea fi considerate ca făcând parte dintr-un R.I. pot fi identificate și în timpul celui de-al doilea război mondial (acțiunile de dezinformare, de intimidare etc). Însă, elernentul de noutate pe care-l aduce astăzi îl reprezintă includerea mijloacelor tehnice sofisticate existente într-o strategie globală, realizată în funcție de scopul urmărit.

Această strategie urmărește obținerea unui avantaj, a unei superiorități informaționale față de adversari sau chiar față de aliați.

Iată câteva argumente care marchează diferențele majore dintre rolul istoric al informației și teoriile actuale privind R.I:

- Superioritatea informațională era o problemă de noroc și nu de sistem. Astăzi, R.I. depinde de o exploatare superioară și sistematică a informației și de diseminarea la timp a acesteia.
- Informația a putut influența anumite *planuri de război,* dar nu și *execuția* lor. R.I. cere o avertizare timpurie și decizii rapide într-un câmp de luptă schimbător.
- Războaiele erau câștigate sau pierdute cu sau fără ajutorul informației. Astăzi, informația este primordială, iar un R.I cere un flux sigur al ei.
- Canalele de comunicare erau în trecut expuse interceptării. In zilele noastre, tehnologia digitală este extrem de

vulnerabilă la interzicerea accesului sau la atacurile care au ca scop manipularea datelor. Atacurile software pot să nu distrugă arme sau forțe, dar pot, cu siguranță, să le interzică sau să le imobilizeze.

Sintetizând, verbele care se potrivesc cel mai bine pentru a rezuma conceptul de R.I. sunt: a capta, a transmite, a trata rapid o informație, a împiedica (adversarul/aliatul să facă același lucru), a denatura, a dezinforma.

Natura deosebit de complexă a R.I. este evidențiată de trăsăturile sale:

- dificultatea precizării adversarilor
- absența unor frontiere de natură geografică și/sau temporală
- multitudinea de ținte
- lipsa unor metode rapide de remediere a consecințelor pe care le generează
- utilizarea unei tehnologii relativ simple, ieftine și larg răspândite
- costurile relativ scăzute ale derulării unui R.I. în raport cu rezultatele ce se pot obține
- posibilitățile sporite de manipulare
- potențialul efectului de bumerang
- ștergerea deosebirilor dintre nivelurile de comandă

Aceste trăsături ale R.I. redimensionează noțiunea de conflict (și competiție) adăugându-i noi atribute: *permanența, transversalitatea și dualitatea.*

- *Permanența* presupune aplicarea unei strategii globale care integrează procesele de colectare, protecție, transport, management și împiedicare a accesului la informație nu numai în perioadele de criză sau conflict.
- *Transversalitatea* semnifică influențarea societății în ansamblul ei și are la bază conceptele de „sistem de sisteme" și „multidisciplinaritate".
- *Dualitatea* se referă la dispariția deosebirilor dintre sfera militară și cea civilă. Statele și forțele armate tind să nu mai

aibă monopolul absolut asupra mijloacelor violente și îndeosebi asupra „violenței informaționale".

La nivel național, centrul strategic de greutate se mută treptat înspre domeniile bancar, financiar, energetic și al sistemelor de distribuție. Infrastructura civilă ajunge cel mai important obiectiv, iar apărarea ei cu forțe convenționale devine problematică.

R.I. este însoțit de noi mijloace de acțiune/influențare care eludează puterea convențională și granițele statelor. Multe dintre aceste mijloace acționează direct la nivelul comenzii și al controlului, al voinței, al informației, precum și asupra elementelor esențiale ale infrastructurii statale.

R.I. vizează structuri ale domeniului politic, economic, social sau militar, nu doar pentru a le distruge sau paraliza ci, mai ales pentru a le influența procesele decizionale. Astfel, se face trecerea de la stadiul de *violență organizată* la stadiul de *influențare ostilă*.

Războiul informațional se manifestă sub două aspecte: *ofensiv* și *defensiv*.

Războiul informațional ofensiv include campanii imagologice, acțiuni psihologice în mediul decizional, sustragerea sau vicierea datelor, introducerea de informații eronate sau false, interzicerea accesului inamicului la datele proprii, distrugerea fizică a elementelor care fac parte din sistemele de comunicații și informatică, acțiuni pe Internet etc.

Războiul informațional defensiv include criptarea, autentificarea și certificarea datelor și a informațiilor, controlul accesului, detectarea și eliminarea software-ului malign, protejarea informativă și contrainformativă, contrapropaganda, contrainducerea în eroare.

In funcție de strategiile de atac-apărare construite și de armele informaționale utilizate, parte din teoreticienii occidentali fac referire la următoarele șapte forme de R.I. [50]

[50] Martin Libicki, "WHAT Is Information Warfare?", National Defense University Press,1995, http://www.ndu.edu/inss/actpubs/act003/a003.html

• *Războiul de comandă și control* (forma exclusiv militară a R.I. - are menirea să anihileze comanda și sistemele de comandă-control ale unui adversar prin integrarea operațiilor psihologice, a securității operațiilor, a inducerii în eroare, a războiului electronic și a distrugerii fizice.

• *Războiul bazat pe informații* (intelligence) - constă în proiectarea, protecția și anihilarea sistemelor care conțin suficiente cunoștințe pentru a domina un spațiu de conflict.

• *Războiul electronic* - utilizează tehnologie electronică și tehnici criptografice pentru dominația spațiului electromagnetic.

• *Războiul psihologic* - utilizează informația pentru a modifica atitudinile și opțiunile aliaților, părților neutre și adversarilor.

• *Războiul hacker-ilor* - constă în atacuri cu software „malign", asupra sistemelor informatice.

• *Războiul în sfera informațiilor economice* urmărește blocarea sau canalizarea informațiilor și crearea unei imagini deformate în scopul obținerii supremației economice.

• *Războiul în spațiul realității virtuale* - folosește Internetul drept cutie de rezonanță și armă de propagandă la nivel mondial.

Acest mod „tranșat" de a prezenta R.I. este contrazis de Daniel Kuehl [51], care consideră mult mai pertinentă îmbinarea tuturor acestor forme pentru a se obține o viziune de ansamblu asupra fenomenului R.I.

In funcție de scopul urmărit, R.I. poate fi purtat [52]:

• *pentru* informație - presupunând managementul unei cantități importante de informații;

• *prin intermediul* informației - vizând transmiterea mesajului dorit sau neutralizarea mesajului adversarului;

---

[51] School of Information Warfare & Strategy. N.D.U.

[52] Jean-Luc Moliner, „La guerre de l'information vue pur un operationnel francais", *L'Anmement*, nr. 60, dec.1997/ian. 1998

• *împotriva* informației - constând în protejarea informațiilor de posibile manipulări

Așa cum am afirmat anterior, particularitatea conceptului de R.I, e dată de realizarea unei strategii integratoare care utilizează mijloace tehnice de ultimă oră.

Integrarea pe care R.I. urmărește să o realizeze apare pe trei niveluri primare. La un prim nivel, R.I. necesită integrarea ofensivei și a defensivei. Dacă se dorește, de exemplu, dezvoltarea metodelor ofensive de R.I., trebuie avută în vedere posibilitatea ca inamicul să poată dezvolta și el, la rândul său, același tip de metode.

Cu alte cuvinte, trebuie evaluate consecințele ce ar putea să apară și metodele de apărare necesare în cazul în care inamicul recurge la aceste metode ofensive. Orice acțiune ofensivă de R.I. trebuie analizată în lumina impactului potențial pe care îl poate avea asupra măsurilor defensive proprii, în timp ce orice acțiune defensivă de R.I, trebuie avută în vedere în lumina impactului asupra potențialului ofensiv.

La al doilea nivel de integrare se află cele șapte forme de război deja menționate. Fiecare dintre acestea are propriile sale bariere, norme, scheme de clasificare și mecanisme de observație. Dar fiecare trebuie integrată, adică planificată, și realizată într-o manieră care să completeze și să îmbunătățească performanțele celorlalte, pentru a atinge obiectivele specifice acelui R.I.

Al treilea nivel de integrare are loc de-a lungul trecerii de la o stare la alta, adică de la pace la criză, apoi la război și înapoi la pace. R.I. are un rol de jucat în fiecare din aceste faze și acesta trebuie conceput în mod coerent.

R.I. se deosebește de atacurile individuale prin faptul că este guvernat de *strategie,* care se concentrează asupra unui *obiectiv.* Strategia constă într-un plan cuprinzător care îmbină armele și tacticile pentru a-și atinge scopul. Armele și tacticile pot fi orice combinație de tehnici, militare sau nu. Obiectivul poate fi militar, politic, economic sau o combinație a acestora.

Astfel, o campanie R.I. poate fi dusă în paralel cu alte operații de luptă, poate fi dusă dincolo de zona de luptă și poate depăși granițele în timp de pace, de criză sau de luptă. Termenul de „informație" în R.I. sugerează faptul că obiectivul unei astfel de campanii implică crearea unor efecte în sfera informațională a adversarului, capabile să-i împiedice sau să-i inspire anumite acțiuni, fapt ce produce un avantaj pentru atacator.

Cunoscând natura războiului informațional, se constată că adevărata țintă a unei campanii R.I. nu sunt sistemele specifice care sunt atacate în momentul respectiv, ci mai degrabă *procesul decizional* al adversarului. Astfel, atacul informațional trebuie să se bazeze nu doar pe caracteristicile acelor sisteme, ci și pe efecte mai mari.

Acest lucru poate fi ilustrat de un exemplu simplu, atacul menit să bruieze un senzor. Ca operație individuală de război electronic, atacul se bazează pe caracteristicile tehnice și operaționale ale senzorului. Ca element al campaniei R.I., planificarea și dirijarea atacului trebuie să se bazeze pe felul în care senzorul contribuie la descrierea situației adversarului și pe informația pe care senzorul o asigură operațiilor și forțelor atacatorului. La un nivel mai înalt, acest lucru trebuie să fie luat în considerare în planificarea atacului, iar implementarea este efectul asupra deciziilor adversarului, blocând, degradând sau falsificând informația senzorului. Același lucru este valabil pentru atacurile asupra sistemelor de comunicare, rețelelor, legăturilor sau centrelor de procesare.

Conceptul general al R.I. poate fi considerat ca având trei părți: un grup de *elemente de R.I.* (tehnici și capacități), o *sinergie globală* care le aplică și le orchestrează și o *țintă*. Doar elementele sunt aceleași în cazul R.I. și al conceptelor tradiționale de atac informațional. O definiție a R.I. trebuie, deci, să descrie obiectivul principal, să identifice și să enunțe elementele aplicabile ale R.I., să arate cum aceste elemente se pot combina în cadrul strategiei de atac al țintei.

Intrucât obiectivele reprezintă sursa pentru crearea unei strategii a R.I, vom începe cu modelul unei ținte. Vom trece în revistă, apoi, câteva dintre elementele utilizate în R.I, pentru ca în final, să prezentăm, prin intermediul unui tabel, organizarea elementelor și relațiile dintre ele.

ȚINTE ȘI ELEMENTE ALE UNUI ATAC INFORMAȚIONAL

După cum remarca Thomas P. Rona, în sfera militară, sistemele informaționale cuprind sistemele de comandă și control, sistemele de *intelligence,* sistemele platformelor de cercetare-lovire și rețelele de comunicații, care constituie infrastructura informațională a sistemelor menționate mai sus.

Sfera civilă posedă și ea echivalentul acestor sisteme critice pentru securitatea națională (centrele de decizie de la nivel politic, economic, religios, social, de exemplu; infrastructura națională: sistemele de alimentare cu apă potabilă, cu energie, cu gaz; sistemele bancare, sistemele de telecomunicație etc). Practic, aceste sisteme informaționale (militare și civile) se sprijină reciproc și, frecvent, utilizează aceeași infrastructură informațională.

Importanța acestor infrastructuri informaționale este evidentă în cazul R.I. Așa cum se remarcă în studiile de specialitate [53] se pot distinge trei niveluri de ținte ale unui atac informațional:

- *Nivelul sistemelor informaționale.* Neglijând obiectivul principal, atacurile R.I. se îndreaptă, deseori, asupra sistemului informațional, care nu întotdeauna reprezintă un sistem electronic. In multe cazuri, acest sistem este ținta inițială a atacului, efectele fiind de natură tehnică (supraîncărcarea sursei de recepție, coruperea datelor, stricarea computerelor,

[53] Scolt Johnson, *Toward a Funcțional Model of information Warfare, http://bss.sfsu.edu/fischer/IR%20360/readings/information%20war.html*

distrugeri fizice etc.). Acest punct este des întâlnit în literatura de specialitate, discuțiile despre RI concentrându-se asupra țintelor și metodelor de atac tehnic. Ceea ce nu se are în vedere este obținerea efectelor operaționale.

• *Nivelul gestionării informației.* Gestionarea informației se referă la transferul informației, răspândirea, stocarea ei. Efectele sunt funcționale: o întârziere a informației sau o schimbare la nivelul capacităților de transfer al informației.

• *Nivelul procesului de decizie.* Efectele operaționale ale atacului R.I. de la acest nivel pot fi indirecte: nu se dorește doar producerea confuziei, ci și formarea, influențarea deciziilor, opiniilor adversarului.

Trebuie observat faptul că efectele de la un anumit nivel generează ele însele efecte la nivel superior. De exemplu, un atac menit să bruieze sistemul de informare blochează sau corupe elementele celui care le primește (efecte tehnice), iar acest lucru reduce informația (efecte funcționale). Efectul operațional ar putea fi întârzierea deciziei.

Scopul final al unei campanii R.I, îl reprezintă nivelul procesului decizional. Așa cum ne sugerează și Thomas P. Rona [54].

Principala sarcină a nucleului este de a transforma, urmând o logică prestabilită sau propria sa logică, stimulii pe care-i primește, în rezultate (comenzi sau mesaje de acțiune către alte nuclee sau către actori externi). Trebuie, de asemenea, observat faptul că nucleul are posibilitatea de a selecta și de a stabili praguri pentru stimuli și de a verifica rezultatul acțiunilor dictate.

Datorită naturii transformatorului logic (fiecare are propria sa experiență, intuiție, cultură și mod de a răspunde la stres) care face foarte dificilă evaluarea modului în care sunt îndeplinite deciziile și datorită multiplelor căi de atac asupra transformatorului logic, problema mijloacelor de protecție și a eficacității lor este deseori prost înțeleasă sau chiar ignorată.

---

[54] În „Information Warfare. An Age-Old Concept with New Insights", publicat în *Defense Intelligence Journal*, 5-1, 1996

Trebuie remarcat faptul că țările industrializate sunt din ce în ce mai dependente de sistemele informaționale. În contextul R.I., acest lucru creează noi vulnerabilități care se adaugă listei vulnerabilităților „clasice" și care repun în discuție conceptul de „securitate națională".

Elementele necesare R.I. sunt:

- tehnicile și capacitățile de atac și de apărare
- strângerea de informații pentru a localiza informația - poziții, forțe, vulnerabilități, apărări
- strângerea de informații pentru avertismente
- strângerea de informații pentru a evalua pagubele

Capacitățile de atac și de apărare sunt funcțiile fundamentale ale R.I. Acestea pot lua forma unor viruși în calculatoare, operații psihologice etc.

Ca orice alt război, R.I. are nevoie de surse externe. Una dintre acestea o constituie strângerea de informații.

R.I. trebuie să fie sprijinit și de o funcție de evaluare a pagubelor și de informații de apărare. Pentru aceasta este nevoie de măsuri pentru a putea detecta și localiza atacurile prin propriul sistem de informare.

Alte elemente-cheie pentru R.I. sunt *expertiza* și *înțelegerea.* Expertiza tehnică e necesară, dar nu și suficientă. O înțelegere a țintei este necesară pentru dezvoltarea unei strategii a R.I.

Orchestrarea numeroaselor elemente ale R.I. este una dintre caracteristicile sale fundamentale. Atacurile combinate sunt aplicate în funcție de specificul țintei.

Pentru a ști cum pot fi combinate și orchestrate diversele elemente ale R.I. trebuie să revenim la modelul țintei. După divizarea țintei pe niveluri, fiecare nivel poate fi divizat la rândul său. Urmează o înșiruire a atacurilor posibile împotriva fiecărui element caracteristic fiecărui nivel. Cunoscând acțiunile și caracteristicile țintei putem identifica capacitățile necesare pentru a conduce fiecare atac împotriva fiecărui element.

Tabelul 1 - Capacităţi specifice R.I.

Elementele ţinta						**Atac/sprijin al acţiunilor**	
Logice				Fizice			
Intlligence		Informaţie		Noduri	Legături		
Fizic	Operaţional	•Date	Control			Ofensiv	Suport
• Locatie • Parametri • Funcţii • Arhitectur • Reţea	•Utilizatori •Flux de date	•Video •Text •Voce •Imagine •Digital	•Stabilirea legăturilor mesajelor •Canal comun de avertlizare	• Surse de date • Schimburi • Fuziunea punctelor • Procesarea punctelor • Strângerea datelor • Convertirea datelor • Interpretare/ • decizie	•Comandă •Date •Calculator	• Blocarea informaţiilor • Coruperea informaţiilor • Saturarea nodurilor • Stergerea informaţiilor • Introducerea informaţiilor • Schimbarea informaţiilor etc.	• Obtinerea de *intelligence* Schimbarea de *intelligence* • Controlul atacului • Utilizarea de *inteligence* etc.

În tabelul 1, legăturile dintre elementele logice și cele fizice nu sunt arătate, iar relațiile dintre atacuri/acțiuni de suport și elementele țintei sunt prezentate mai puțin sub formă de concepte. Tabelul nu prezintă nivelurile secundare. Fiecare element poate fi divizat la rândul său. Tabelul nu arată acțiunile de apărare și relațiile lor cu acțiunile de atac.

In tabel, termenul „intelligence" se referă la informația care descrie elementele țintei. De reținut că există două tipuri de intelligence: fizic și operațional. Intelligence-ul fizic asigură parametrii țintei și informația structurală sau arhitecturală a rețelelor urmărite. Intelligence-ul operațional identifică utilizatorii.

Categoria „informație" este divizată în „date" (informația pe care adversarul o interpretează) și „controlul informației".

Atacurile asupra controlului informației pot fi o amenințare serioasă la adresa rețelelor de comunicare. Categoria „date" este divizată în tipuri, căci acestea definesc capacitățile tehnice necesare pentru atac.

Acțiunile de atac includ măsuri ofensive și defensive, după cum arată tabelul. Măsurile de atac nu se limitează la blocarea și coruperea informațiilor. Cineva poate introduce informații false în sistemul de informare al adversarului. Cineva poate utiliza sau nu informația obținută de la adversar, cum indică denumirea „schimb de informații". Funcția „utilizarea informației" se referă la exploatarea informației colectate.

Tabelul este un ghid general și nu o descriere strictă. Nu toate sistemele de R.I. sau atacurile de R.I. conțin elementele din tabel. Acesta oferă un cadru de lucru pentru căutarea și interpretarea capacităților și pentru evaluarea unui R.I.

INFRASTRUCTURILE CRITICE ÎN RĂZBOIUL INFORMAȚIONAL

Când se vorbește de orientarea spre țintă în contextul R.I., se fac, de obicei, analogii directe cu războiul cinetic, specific

erei industriale: atacuri asupra infrastructurii critice, atacuri asupra sistemelor de comandă și control etc. Acum sunt avute în vedere și atacurile asupra computerelor și sistemelor informaționale.

La nivelul strategic al analizei, sectoarele infrastructurii critice reprezintă „organele vitale" ale societății. În era informațională, problema care se pune este aceea dacă aceste aspecte ar trebui sau nu să intre în responsabilitatea armatei.

Acestea nu numai că sunt esențiale bunăstării economice ale oricărei societăți evoluate, ci și din ce în ce mai importante pentru viabilitatea forțelor armate ale țării respective. Sectoarele civil și militar se suprapun din ce în ce mai mult. Sectoarele infrastructurii critice includ:

- sistemele și rețelele de comunicații terestre și spațiale
- sistemele și rețelele de transport
- sistemele și rețelele de distribuție a energiei
- sistemele bancar și financiar
- sistemele de distribuție, rafinare și purificare a apei
- serviciile guvernamentale esențiale
- serviciile de urgență (poliție, pompieri, salvare)

În societățile evoluate aceste servicii sunt o responsabilitate împărțită de către sectoarele public și privat. Dar indiferent de cine le gestionează, aceste sectoare ale infrastructurii au în comun un element esențial: faptul că sunt informatizate într-o măsură din ce în ce mai mare. Progresele în materie de informatică au fost folosite pentru îmbunătățirea și eficientizarea serviciilor infrastructurii și pentru reducerea costurilor operaționale, însă, pe măsură ce se favorizează eficiența infrastructurilor critice, se mărește și vulnerabilitatea lor.

Referitor la protecția infrastructurii critice, trebuie luate în considerare patru aspecte ale amenințării: riscul sinergie (1), amenințarea asimetrică (2), amenințarea asincronă (3) și criza de încredere (4).

1) Statele-națiune sunt, în principiu, „sisteme de sisteme" elaborate și complexe. Cu cât națiunea este mai avansată din

punct de vedere economic, cu atât relațiile infrastructurii sunt mai complexe. Distrugerea sau afectarea gravă a sectorului infrastructurii critice are imediat efecte adverse asupra celorlalte sectoare, și nu doar la nivel național, întrucât sistemele și sub-sistemele infrastructurii sunt interdependente într-o măsură din ce în ce mai mare, ele nu pot fi segregate sau izolate într-un efort de limitare a pagubelor.

2) Preocuparea pentru *amenințările asimetrice* la nivel strategic și tactic este deosebit de relevantă pentru aspectul protecției infrastructurii. O putere mai mică (statală sau nonstatală) poate produce mari pagube unei națiuni mai robuste, dată fiind dependența sporită a acesteia din urmă de infrastructurile critice. Altfel spus, o societate mai puțin dezvoltată este mai puțin dependentă de aceste sisteme atât fizic, cât și psihologic.

3) O *amenințare asincronă* poate fi și ea o problemă pentru societățile dependente de o infrastructură sofisticată. Atacul fizic asupra unor centre critice pentru societate are efecte vizibile. Dar pot exista și atacuri punctiforme asupra sistemelor infrastructurii critice, repetate și extinse pe parcursul unei perioade mai lungi de timp, fără un model exact și fără un autor imediat identificabil, care pot pune în pericol siguranța națională.

4) O problemă îngrijorătoare pe care o ridică o campanie susținută de atacuri asimetrice la adresa infrastructurii este *criza de încredere publică* ce poate rezulta. Se poate crea iluzia că instituțiile publice și cele private sunt incapabile de a asigura bunăstarea indivizilor.

Aceste lucruri nu sunt menite să descrie un viitor apocaliptic. Vor doar să sublinieze gravitatea provocării. Problema pe care o reprezintă protecția infrastructurii critice este aceea că în societățile dezvoltate din punct de vedere economic sectoarele public și privat sunt doar semicompatibile.

Acestea au scopuri diferite, motivații diferite, responsabilități diferite și „produse" diferite. Provocările pe care le ridică cooperarea dintre aceste sectoare se bazează pe trei aspecte: transmiterea informațiilor (1), aspecte legale (2) și provocările tehnice (3).

1) Dificultățile *transmiterii informațiilor* își găsesc originea la nivelul percepțiilor și încrederii. De cele mai multe ori, sectoarele public și cel privat nu au încredere deplină unul în celălalt. În mod cert, companiile din cadrul aceluiași sector comercial al infrastructurii nu sunt caracterizate de o încredere reciprocă, în ciuda acordurilor de parteneriat. Există date confidențiale privind anumite proceduri și vulnerabilități. Pe de altă parte, guvernul, și în special sectorul de apărare și securitate națională, este interesat de informațiile clasificate, iar legile și regulamentele limitează transmiterea și diseminarea acestora.

Odată ce transmiterea informațiilor este considerată necesară, ce tipuri de informații trebuie să circule între sectorul public și cel privat, pe de-o parte, și în cadrul sectoarelor infrastructurii, pe de altă parte? Datele și analizele privind amenințările trebuie transmise. Dar ce se întâmplă cu datele și analizele privind vulnerabilitățile, care se desprind din cele dintâi? Acesta este un aspect foarte delicat.

2) Aspectele legale sunt și ele o problemă. În cadrul sectorului privat există preocupări pentru situații precum antitrustul. Există apoi o serie de aspecte legale internaționale care depășesc aria de interes a unui stat-națiune.

3) Există, de asemenea, o serie de aspecte tehnice care complică procesul colaborării dintre sectoarele public și privat în protecția infrastructurii. Acest lucru se aplică mai ales în domeniul tehnologiei informaționale, iar procesele rezultante de „e-business" și „e-commerce" schimbă natura întregului sector privat. Pentru acesta din urmă, viteza afacerilor este principalul motor. Afacerile se dezvoltă și se adaptează azi

mai rapid decât o va face vreodată guvernul. Această dezvoltare rapidă este posibilă numai în absența intervenției guvernamentale. Inovația tehnologică provine aproape în exclusivitate din sectorul privat. Iată de ce problema colaborării public-privat în protecția infrastructurii critice se complică.

Așa cum am afirmat de la început, societățile avansate se îndreaptă către o sferă nouă, indiferent că aceasta se numește sferă informațională sau ciberspațiu. În acest demers, omenirea va aduce cu ea vechile ei nevoi și impulsuri: nevoia de a comunica, de a conversa, de a comercializa. Ea va aduce cu ea și impulsul către violență, conflict și război. Iar în procesul acestei migrări, se vor dezvolta și necesități, impulsuri și obiceiuri noi. Printre acestea se află și nevoia de protecție a infrastructurilor critice (fizică și informațională).

PROBLEMATICA EVALUĂRII AMENINȚĂRILOR

Imaginația este mai importanta decât cunoașterea
Albert Enstein

De multe ori discuțiile privitoare la amenințările de tip R.I. se poartă în jurul războiului informatic, în mod special pe marginea vulnerabilității calculatoarelor și a rețelelor. Dacă acceptăm modelul teoretic al lui M. Libicki în care R.I. înseamnă integrarea a șapte forme de război, focalizarea pe calculatoare este incompletă și de neînțeles. O amenințare de tip R.I. ridică, într-adevăr, întrebarea dacă mediul nostru informațional poate fi manipulat de alții pentru a câștiga superioritate informațională, inclusiv utilizând calculatoarele, dar fără a se limita doar la acestea.

Amenințările R.I. sunt prezente la toate nivelurile (nivelul sistemelor informaționale, al gestionării informației și al procesului de decizie) și, în același timp, sunt multidimensionale, având o dimensiune politică, economică,

culturală, juridică și nu doar una pur militară, cum greșit se crede. [55]

Așa cum este ilustrat și în figura *2*, amenințarea poate fi clasificată în mai multe tipuri, fiecare putându-se „activa" în momentul în care întâlnește unul dintre elementele unui sistem. Pentru a avea succes este necesar ca cel care lansează atacul informațional să cunoască foarte bine arhitectura sistemului, modul în care se iau deciziile și transformatorul logic utilizat (nucleul care ia decizii), lucru nu foarte ușor de realizat.

Măsurile de protecție împotriva amenințărilor R.I. trebuie să aibă la bază evaluarea amenințărilor și avertizarea timpurie.

Evaluarea amenințărilor trebuie, inevitabil, să ia în considerare vulnerabilitățile. O evaluare completă a riscurilor trebuie să suprapună amenințările potențiale și cele identificate cu vulnerabilitățile sistemelor informatice, pentru a determina nivelul de risc și a putea planifica răspunsuri.

O amenințare este o combinație de capacități și motive. Puterea unui adversar a fost măsurată până acum în termeni de capacități militare și diverse alte elemente care puteau fi convertite în capacități militare, cum ar fi: puterea economică, populația și teritoriul. Indexul compus al capacităților este un exemplu clasic în această abordare, agregând elemente cuantificabile din domeniile militar, industrial și demografic pentru a construi un indicator al puterii naționale.

Un factor ce trebuie luat în considerare este acela că sistemele de evaluare ale amenințărilor la adresa securității naționale și militare au fost în mod tradițional dezvoltate pentru a evalua capacitățile unor organizații similare din „tabăra adversă". Din acest punct de vedere, ambele părți erau organizații cu structură ierarhică, funcționând pe baza unor structuri și modele ușor de înțeles, în epoca R.I, organizațiile de tip rețea, prin natura organizării lor, constituie amenințări la fel de importante ca și cele de tip ierarhie.

---

[55] O prezentare interesantă a amenințărilor R.I. a fost făcută de David Alberts în *Defensive Information Warfare*, N.D.U., 1996. D. Alberts clasifică amenințările în trei categorii: amenințări de zi cu zi, amenințări potențial strategice și amenințări strategice, în funcție de aria pe care o acoperă și de gravitatea consecințelor lor.

Elemente ale unui sistem	**Amenințări generice**							
	Distrugere	Scoatere din funcțiune	Interferență	Înșelătorie	Saturare	Intruziune	Întârziere	Exploatare
Observabile		?	?	?				
Sursele mesajului	?			?				?
Comunicații	?		?		*		?	
Managementul rețelelor de comunicație		*						
Șef		?		*	?		*	
Echipă/Experți		?		*	?		?	
Modele de decizie				?	?			
Procesori		?						
Bază de date	?			?				

*Figura 2 - **Amenințări** generice versus elemente importante ale unui sistem*

Motivațiile sau intențiile acestora sunt mult mai dificil de evaluat decât capacitățile atât pentru analistul de *intelligence*, cât și pentru factorul de decizie.

Evaluarea amenințărilor specifice R.I., provenite din mediul substatal, produce cu greutate rezultate clare. Este dificil să acorzi valori clare diferiților indicatori utilizați și ar fi, poate, mai utilă folosirea unor metode care să permită cuantificarea prin intermediul unui interval de valori.

RĂZBOIUL INFORMAȚIONAL ȘI LEGISLAȚIA INTERNAȚIONALĂ

Dezbaterile asupra problematicii războiului informațional au scos deseori în evidență problemele tehnologiei moderne, fără a lua însă în discuție mediul legal internațional în care se manifestă epoca informațională.

Examinarea relației dintre războiul informațional și legislația internațională presupune, inevitabil, explorarea câtorva probleme caracteristice: ce reprezintă „războiul" în epoca informațională și ce tipuri de activități pot fi numite „război informațional"? Ce este un act de „război informațional"? Ce devin „forța", „atacul armat" sau „agresiunea armată" într-o eră a informației? In ce mod sunt sau pot fi afectate noțiuni ca „suveranitatea națională", „inviolabilitatea frontierelor"?

Războiul informațional ridică câteva provocări importante legislației internaționale actuale.

În primul rând, legile internaționale definesc starea de război și starea de pace. Pentru a face această distincție, nivelul și natura pagubelor este un criteriu. Pagubele produse de atacurile informaționale pot fi diferite de cele create de un război tradițional. Pentru a lua un exemplu, distrugerile cauzate de bombe sunt ușor de observat, în vreme ce alterarea sau manipularea sistemelor informatice pot produce pagube

intangibile, cum ar fi o perturbare a serviciilor de orice natură și chiar a societății, în final. Acest lucru întărește convingerea că războiul informațional este capabil să șteargă linia incertă, din punct de vedere filosofic, dintre război și pace.

În al doilea rând, până în prezent, statele au constituit subiectul major al legislației internaționale. Statele sunt entități care posedă o autoritate suverană asupra unui anumit teritoriu. Însă posibilitatea semnalelor, de exemplu, de a traversa rețele internaționale pune în discuție conceptul de suveranitate teritorială națională, principiu fundamental al relațiilor internaționale de la Tratatul de la Westfalia, din 1648, care stabilește faptul că fiecare națiune are o autoritate exclusivă asupra evenimentelor care se petrec în interiorul granițelor sale.

Noutatea tehnologiilor ar putea explica absența oricărei măsuri de prevedere explicită în legislația internațională care să interzică practicile ce țin de fenomenul cunoscut sub denumirea de „război informațional". Absența unor astfel de măsuri este importantă, căci, în general, ceea ce legislația internațională nu interzice, este permis. Pe de altă parte, inexistența acestora nu este hotărâtoare, deoarece chiar dacă legislația internațională nu se referă direct la anumite arme sau tehnologii, principiile sale generale pot fi aplicate și în cazul acestora.

Conform tratatelor internaționale și a cutumei, teritoriul statelor neutre este inviolabil de către forțele beligerante, în cazul unui conflict, încălcarea frontierelor naționale, în legislația internațională actuală, se referă în special la acțiunile fizice realizate. Nu se știe, însă, dacă un atac realizat printr-o rețea care traversează un teritoriu neutru sau utilizează sateliți, calculatoare sau rețele aparținând unor state neutre are aceeași valoare juridică ca aceea a unei incursiuni a unor trupe înarmate [56].

Astfel de atacuri sunt dificil de încadrat, în momentul de față,

[56] *U.N. Manual on the Prevention and Control of Computer-Related Crime.* 261-264, 1993

de legislația internațională. Războiul, în accepțiunea tradițională, presupune forțe înarmate și violență. Articolul 2 (4) al Cartei O.N.U. interzice amenințarea sau utilizarea forței împotriva integrității teritoriale și independenței politice a statelor. Insă un atac informațional reprezintă o „utilizare a forței"? Ce înseamnă „forță"? Aceasta, din perspectiva articolului 2 (4), este privită ca „forță armată". Din acest punct de vedere, ne putem întreba dacă un atac informațional este o „utilizare a armelor".

Carta O.N.U. conține două importante excepții de la regulă, care permit utilizarea forței armate. Este vorba, în primul rând, de utilizarea forței având autorizația expresă a Consiliului de Securitate și, în al doilea rând, de utilizarea forței ca măsură de autoapărare.

Capitolul al VII-lea al Cartei permite Consiliului de Securitate să autorizeze utilizarea forței de către state, în cadrul coalițiilor formate ad-hoc sau în cadrul organizațiilor regionale după ce s-a stabilit că este vorba de o „amenințare a păcii", de o „ruptură a păcii" sau de un „act de agresiune".

Întrebarea care apare natural este aceea dacă un atac informațional poate fi considerat o „amenințare a păcii", o „ruptură a păcii" sau un „act de agresiune", având în vedere caracterul său diferit de cel al unui atac fizic.

Adunarea Generală a O.N.U. a definit „agresiunea" plecând de la o viziune tradițională a războiului [57]. Declarația definește „agresiunea" pe care Consiliul de Securitate este autorizat să o constate [58] drept „utilizarea forțelor armate de către un stat împotriva suveranității, integrității teritoriale sau independenței politice ale unui alt stat sau într-o cu totul altă manieră incompatibilă cu Carta O.N.U. [59] Categoria armelor informaționale

[57] Adunarea Generală, Rezoluția 3314, *Declaration on Agression, din* 14.12.1974.

[58] *Carta Națiunilor Unite.art.3.* www.icj-cij.org/cijwww/cdocumentbase/Basetext/cunchart.html.

[59] *Declaration on Agression*, art.1 din 14.12.1974.

ar putea fi acoperită de fraza: (...)„utilizarea oricărei arme împotriva teritoriului unui alt stat"[60]. Un atac informațional având ca miză „suveranitatea, integritatea teritorială sau independența politică" ar putea fi considerat un „act de agresiune" care să determine Consiliul de Securitate să ia poziție.

A doua excepție de la regulă o constituie acceptarea utilizării forței ca mijloc de autoapărare. Articolul 51 al Cartei recunoaște dreptul inerent la auto-apărare al statelor în caz de „atacuri armate". Sunt însă atacurile informaționale „atacuri armate"?

Dificultatea caracterizării anumitor forme ale războiului informațional ca elemente de „forță", „război" sau „agresiune", din punct de vedere al dreptului internațional, nu presupune implicit și imposibilitatea instituțiilor internaționale de a răspunde la astfel de fapte. Capitolul VII al Cartei O.N.U., de exemplu, acordă Consiliului de Securitate autoritatea și responsabilitatea de a determina existența oricărei „amenințări a păcii" sau a oricărui act de agresiune"[61] și de a decide maniera de a răspunde la acestea"[62]. Din această perspectivă, multe dintre atacurile informaționale ar putea fi considerate „amenințări ale păcii" și, în consecință, ar putea deveni subiecte ale deciziilor Consiliului de Securitate.

Încercările de revizuire a unor aspecte ale legislației internaționale, care să surprindă mai temeinic fenomenul războiului informațional, se fac timid simțite. Federația rusă, de exemplu, caută să inițieze un curent favorabil punerii la

[60] Art.3 (b) al Rezoluției *3314, Declaration on Agression, din* 14.12.1974

[61] *Carta Națiunilor Unite*, art. 39, www.icj-cij.org-cijwww-cdocumentbase-Basetext-cunchart.html

[62] *Carta Națiunilor Unite*, art. 41- 49, www.icj-cij.org-cijwww-cdocumentbase-Basetext-cunchart.html

punct a unei legislații internaționale în privința războiului informațional [63].

Societatea informațională, dincolo de beneficiile pe care le aduce cu sine, ridică probleme importante. Guvernele se confruntă cu probleme fundamentale cum ar fi cele care privesc modul în care se pot garanta valorile democratice într-o societate informațională. Frontiera dintre starea de pace și cea de război este tot mai greu de identificat. Unde începe și unde se termină pacea? Aceasta n-ar putea fi doar un război insesizabil?

Pentru moment există opinii numeroase și diferite privind necesitatea surprinderii la nivelul legislației internaționale a activităților informaționale și maniera în care acestea pot deveni subiecte ale dreptului internațional, dat fiind că fiecare dintre acestea este motivată de interesele proprii.

În ciuda acestei stări de fapt, nu se poate trece cu vederea faptul că noțiunea de „război", așa cum este ea definită de Carta O.N.U., tinde să devină o noțiune depășită de evenimentele timpului nostru. Carta nu evoluează în același ritm cu realitățile de azi și tinde să ofere tot mai greu o imagine adecvată a lumii actuale.

---

[63] In acest sens, Federația Rusă a prezentat la a 53-a Sesiune a Adunării Generale un proiect de rezoluție privind *„Realizările spațiului informatizat și al telecomunicațiilor, în contextul securității internaționale"*. Proiectul de rezoluție invita statele membre O.N.U. să își exprime un punct de vedere asupra utilizării tehnologiilor informatice în scopuri militare, asupra definiției conceptelor „arme informaționale" și „război informațional", asupra oportunității elaborării unor norme juridice internaționale privind utilizarea armelor informaționale, asupra necesității creării unui sistem internațional de monitorizare a amenințărilor legate de securitatea informatică și de sistemele de telecomunicații (a 53-a Sesiune a Adunării Generale, 08.09-18.12.1998, punctul 64 pe ordinea de zi *„Menținerea securității internaționale: Prevenirea degradării violente a Statelor")*.

VULNERABILITĂȚI ALE TEHNOLOGIEI INFORMAȚIEI

MAARTEN VELTMAN*
RICHARD L. PARKER**

Toate sistemele de tehnologia informației și comunicației (ICT) au vulnerabilități. Slăbiciunile acestor sisteme sunt introduse în timpul uneia din fazele de stabilire a specificațiilor, implementării sau fazei operaționale. Lăsând deoparte faptul că aceste vulnerabilități pot aveaun caracter intenționat sau neintenționat, trebuie luat în considerare că acești factori fac ca securitatea informației să fie la fel de puternică ca legăturile ei cele mai slabe.

O echipă de profesioniști – o echipă roșie – are ca scop combinarea capacităților tehnice necesare cu practica în vederea identificării și evaluării acestor vulnerabilități. Primul pas în desfășurarea analizelor efectuate de echipa roșie este culegerea de informații urmată de analize pe zone (site), rezultând un raport complet și accesibil. Mijloacele și tehnicile utilizate de cele mai performante sunt aceleași cu cele utilizate de hackeri în prezent pentru sisteme de calcul și rețele de calculatoare.

Experiența dovedește că dezvoltarea de metode și menținerea unei legături de cooperare cu personalul responsabil sunt cruciale pentru formarea unei echipe roșii profesioniste.

Toate sistemele de tehnologia informației și comunicației (ICT) au vulnerabilități. Odată ce un calculator sau o componentă rețea este introdusă într-un sistem, vulnerabilitățile acelei

* Laboratorul de fizică și electronică, Olanda.
** Agenția NATO Haga, Olanda.

componente expun restul sistemului la riscuri. Există în mod normal trei surse care generează puncte slabe în sistemele de securitate - specificare, implementare și operare.

Punctele slabe specifice specificării și implementării sunt de obicei identificate prin experiență sau analize de laborator și se concretizează în petece *(patch-uri)* sau actualizări (*upgrad*-ări). Dar chiar și cel mai sigur sistem poate să aibă vulnerabilități introduse prin practici defectuoase de operare/configurare.

Cele mai moderne sisteme de ICT au posibilități de comunicare și aplicare bazate pe setul de protocoale TCP/IP. La momentul specificării lor, aceste protocoale nu au abordat aspectele de securitate așa cum le cunoaștem noi astăzi; ele au fost proiectate pentru a fi utilizate într-o comunitate de conectare restrânsă unde toți membrii aveau încredere unul în celalalt.

Există unele aspecte ale acestor protocoale care sunt în prezent puțin problematice. Protocolul de transfer al fișierelor (FTP), de exemplu, nu numai că permite obținerea unui fișier prin conectare la distanță, dar de asemenea permite unui utilizator conectat la distanță să șteargă și să înlocuiască fișiere de pe server. În mediul specific zilelor noastre, trebuie luate măsuri pentru a asigura că numai utilizatori de încredere conectați la distanță au aceste capabilități, altfel modificarea web-site-ului ar fi un element mult mai cunoscut decât este în realitate.

Implementarea vulnerabilităților poate fi neintenționată sau intenționată. Vulnerabilitățile neintenționate sunt destul de cunoscute - inadvertențe software *(bug-uri)*. Uneori, aceste inadvertențe conduc către breșe de securitate posibile (ex. depășirea de memorie generează blocarea unui program într-o zonă temporară privilegiată, rezultând o încălcare a drepturilor de acces) sau uneori pot genera comportamente nedorite (ex. blocări ale ecranului). În oricare din cazuri inițiatorii nu au dorit ca aceste manifestări să aibă loc și când o astfel de inadvertență este descoperită, apare foarte repede un petic sau o modificare a programului pentru a corecta problema.

Implementarea intenționată a vulnerabilităților este cu totul altă problemă. În unele cazuri acestea pot fi de tipul „ușa din spate" sau „cal troian" lăsate în urmă pentru a permite programatorului să exploateze funcții ascunse dintr-o anumită componentă de echipament. Un exemplu uzual a acestui tip de cod este omniprezentul „*Easter Eggs* - Ouă de Paști". Ouale de Paști reprezintă în mod curent un cod nedăunător lăsat în urmă de inițiatori și este invocat de un anumit trigger de intrare (filtru de interogare) sau trigger eveniment; funcționalitatea pe care o reprezintă nu are nimic de-a face cu funcția declarată a programului.

Având astfel identificată cu grijă locația oului în cadrul modulului executabil, modificarea sau înlocuirea codului ar putea fi realizată fără o diferență observabilă în operarea programului și fără modificarea dimensiunii fișierului. Este ingrijorător faptul că cineva ar putea șterge codul Oului Estic și să-l înlocuiască cu ceva dăunător, cum ar fi un modul de modificare sau redirectare a datelor la salvarea fișierelor.

O parte a problemei stă în practica standard de furnizare a configurațiilor implicite pentru sisteme ce le fac cât mai ușor de activat și rulat. În scopul de a spori posibilitatea componentelor sistemului de a opera „potrivit specificațiilor", configurațiile implicite sunt proiectate pentru a fi cât mai „tolerante" posibil - permițând cea mai largă variație a condițiilor în care componenta va opera. De exemplu, o stație Sun Sparc este configurată în mod uzual pentru a accepta un domeniu larg de servicii rețea (ex. email SMTP și sistemul de fișiere în rețea (NFS)).

Uneori configurațiile acceptă funcții de securitate ce nu sunt integrate suficient în sistemul de operare existent. De exemplu, nu este de nici un folos dacă elementele de securitate cum ar fi conectarea și verificarea sunt instalate, dacă ieșirea nu este niciodată verificată sau utilizată de personalul autorizat sau funcțiile automate. Un alt exemplu larg răspândit este utilizarea de parole slabe (sau neexistente) pe timpul procesului de

identificare și autentificare *(login)*. Exemple ca acestea fac operatorii să se întrebe de ce elementele „de securitate" au fost instalate pe primul loc.

Chiar atunci când o componentă sistem este configurată inițial pentru a reduce numărul de vulnerabilități, configurația componentei se modifică în timp. Sunt instalate noi pachete software și sunt făcute actualizări de sistem; utilizatorii și operatorii modifică parametrii pentru a aduce schimbările corespunzător cerințelor operaționale. Mai departe, mulți din acești parametrii nu sunt independenți și astfel schimbările pot introduce efecte colaterale neprevăzute. Toate aceste aspecte combinate fac aproape imposibilă estimarea în ansamblu a posturii de securitate a unui sistem ce cuprinde un mare număr de servere, stații de lucru și componente de comunicații.

În ultimii ani, specialiștii în securitatea informației (InfoSec) au început să se bazeze tot mai mult pe o tehnică de analiză numită „echipa roșie". Numele este împrumutat din exercițiile militare curente unde forțele gazdă au asociat indicativul de „echipa albastră" și forțele opuse au asociat indicativul de „echipa roșie". Prin jucarea scenariului împotriva unui „inamic" activ, tacticile și strategiile pot fi revăzute și rafinate. În lumea ICT, sistemele operaționale sunt revizuite pentru vulnerabilități de securitate de o echipă de specialiști de InfoSec, utilizând mijloace și tehnici speciale dezvoltate pentru aceasta, și uneori împrumutate de la adversarii potențiali – *hackeri*.

Restul acestui articol detaliază natura echipei roșii InfoSec, tipurile de mijloace și tehnicile implicate, felul rezultatelor ce pot fi obținute și unele observații bazate pe experiența de echipă roșie.

La sfârșitul anului 1993, Dan Farmer și Wieste Venema au realizat lucrarea intitulată „Îmbunătățirea securității site-ului dvs. prin pătrunderea în el".

Lucrarea a avertizat operatorii să înceapă să analizeze securitatea sistemelor lor prin abordarea acestora din punctul de vedere al hacker-ilor. Această lucrare a anunțat de asemenea

realizarea unui produs denumit Sistemul de Administrare a Securității pentru Analiza Rețelelor, prescurtat SATAN. SATAN automatizează o serie de verificări de vulnerabilitate realizate în mod curent în sistemele Unix.

El s-a bazat pe munca prealabilă făcută de Farmer pentru COAST și CERT (COPS - Calculator Oracle și Sistemul de Parole) și munca prealabilă a lui Venema, incluzând filtre TCP. Lucrările "Există dragoni" și „Pachete găsite pe Internet" scrise de Steve Bellovin au detaliat traficul rețea asociat cu încercarile hacker-ilor, cartea lui Bellovin și Cheswick „Ziduri de foc și securitatea Internet: interviu cu hacker-ul Willy", sunt câteva lucrări și numeroase eforturi contemporane au condus la stadiul curent al practicii în domeniul analizelor vulnerabilității de rețea/ sistem, bazate pe sisteme de probă pentru vulnerabilități cunoscute sau suspectate „din afară", utilizând tehnici de exploatare pentru determinarea posturii de securitate a sistemelor țintă.

Aceste documente și activitățile pe care ele le reprezintă formează baza analizelor de securitate a sistemelor ICT bazate pe scanarea activă a vulnerabilităților exploatabile - echipa roșie. Echipe de specialiști care dispun de mijloace hardware și software special construite pot oferi în acest mod analize independente a posturii de securitate a sistemului.

În timp, personalul, metodele și tehnicile pentru realizarea acestui tip de analize de vulnerabilitate au devenit mai specializate, migrând de la sisteme de operare, la roluri dedicate în analizele de vulnerabilitate. Din nou, împrumutând tehnologia din domeniul militar și dorindu-se, în parte, adoptarea acestor tehnici de către organizațiile militare cum ar fi Agenția Sistemelor Informaționale ale Apărării (DISA), și Centrul de Război Informațional al Forțelor Aeriene (AFWIC) în SUA, acest proces a devenit cunoscut ca „echipa roșie".

Formarea și utilizarea unei echipe roșii nu este totuși o problemă simplă. Găsirea membrilor în echipă cu capabilități tehnice corespunzătoare poate fi dificil de realizat. Mijloacele

necesare pentru acest tip de activitate pot fi scumpe și nu întotdeauna îndeplinesc așteptările. Personalul responsabil pentru asigurarea securității sistemelor este posibil să nu aprecieze venirea unei echipe care să prezinte zonele in care sistemul este deficient. Orice element subiectiv poate să influențeze eforturilor de analiză: conflicte de personalitate, interpretarea greșită a rezultatelor etc.

Formarea unei echipe poate să fie prima provocare reală. Persoanele implicate în acest tip de activitate sunt de obicei cele cu indemânări tehnice performante, cu un larg spectru de cunoștinte in domeniul tehnicii de calcul, a protocoalelor de comunicații. Cei mai mulți au experiență în dezvoltarea și/sau operarea câtorva din aceste componente. O condiție necesară este „nevoia de a cunoaște" cum lucrează sistemele, de jos până la nivelul de înțelegere a structurilor de date și a secvențelor de interschimb specifice proceselor de IT.

Aceste caracteristici (diversitatea și puterea personalităților ce le însoțesc de obicei) au făcut dificilă asamblarea mai multor grupuri de analiști capabili de a realiza analize de tipul „echipă roșie". Din fericire, uneltele și tehnicile sunt disponibile mai structurat, făcând posibilă instruirea personalului mai puțin orientat tehnic în ceea ce se utilizează ca fiind ceva de adevărată artă mai curând decât o practică binedefinită.

Cât timp un grad acceptabil de abilitate tehnică este necesar pentru a aplica complet uneltele și tehnicile și pentru interpretarea corespunzătoare a rezultatelor, înțelegerea îndeaproape a modului de lucru intern a componentelor de IT nu mai este necesară. Specialiștii InfoSec cu o înțelegere detaliată a structurii interne a sistemelor de IT sunt persoane necesare pentru analize și contramăsuri la vulnerabilitățile noi și complexe precum și pentru furnizarea de sfaturi pentru echipele roșii operaționale. Selecționarea și familiarizarea cu „unelte de cumpărăt" devine următoarea provocare majoră.

Pentru cea mai mare parte, aceste unelte colectează împreună vulnerabilități și exploatări cunoscute, automatizează sarcina de

verificare a sistemului și necesită o mai slabă înțelegere a tuturor detaliilor despre toate vulnerabilitățile din partea utilizatorilor.

Unele dintre aceste unelte sunt dezvoltări comerciale (ex. Analiza de Securitate Kane), unele sunt disponibile gratuit (ex. Scotty/Tkined, NTCrack) și unele sunt câte puțin din ambele (ex. ISS Internet Scarmer oferă atât o versiune gratuită limitată cât și o versiune comercială cu toate capabilitățile).

Tabelul de mai jos prezintă un scurt subset de unelte utilizate pentru a detecta și corecta (sau exploata) vulnerabilități în sisternele de operare și aplicații larg răspândite în componentele de comunicații din zilele noastre, stații de lucru și servere. Uneltele au fost grupate pentru simplificarea înțelegerii capabilităților lor generale. Sublinierile n-ar fi trebuit plasate pentru stabilirea categoriilor lor ci ar trebui să se concentreze pe înțelegerea posibilităților și aplicațiilor lor.

Analize de vulnerabilitate
Internet Scarmer, Kane Security Analist, Trident IP Toolbox/ L3 Expert, Security Profile Inspector (SPI), NAI CyberCop, SATAN
Monitorizare rețea
Sniffer, Etherpeek, TCPDump, Snoop, IPWatcher, T-sight, Scotty/Tkined
Detectare intruși
NetRanger, Stalker, Intruder Alert, Network Flight Recorder
Exploatare
Crack4, Offline NT Password Utility, NTCrack, CDC Back Orifice
Altele notabile
Ted wrappers, Tripwire, COPS, crack, ScarmT, Nmap port scarmer

Tabelul 1: *Unelte de tip „echipă roșie"*

O dată ce echipa a fost constituită și uneltele selectate, începe adevărata parte dificilă - obținerea acceptării comune și domeniul de experiență. Cât timp activitatea de laborator este necesară, nu există substitut pentru experiențe operaționale. Învățarea cum trebuie rulat și analizat cu întreruperi minimale și efect maxim nu

este un exercițiu abstractă, reprezintă cunoștințe obținute prin experiență.

Tipurile de vulnerabilități care pot fi găsite de către echipele roșii sunt diverse. Ele diferă de la probleme tehnice, organizaționale, la probleme sociale și în unele cazuri ele se suprapun.

Începând cu o perspectivă tehnică o structură uzuală de rețea poate fi recunoscută. Cele mai multe rețele care sunt în atenția echipelor roșii constă din aceeași structură rețea și aceleași elemente de rețea. La nivel fizic vor exista cabluri de rețea și fire care fac posibilă comunicarea între elementele rețelei. Router-ele și comutatoarele oferă un mijloc de canalizare a traficului dintr-un loc într-altul. Mai mult vor exista sisteme ce oferă servicii pentru stații de lucru sau clienți.

Acționând ca un utilizator de nivel mediu cineva n-ar putea să aibă grijă de toate aceste elemente, mai puțin în situația în care ele nu sunt funcționale. Din perspectiva utilizatorului, serviciile cele mai uzuale ar trebui să fie poșta electronică, accesul la fișiere, interogarea web și posibilitatea de a participa la noile discuții (ale organizației).

Luând aceste servicii generalizate ca o bază, cineva poate uita ușor că există o mulțime de protocoale în spate care fac posibile aceste servicii. De exemplu, protocoalele ce facilitează serviciul de poștă electronică este Protocolul de Transfer al Poștei Simple (SMTP), Protocolul Post Office (POP) și Protocolul de Acces al Mesajelor Internet (WAP). Lăsând deoparte standardele și protocoalele afiliate cu aplicația de poștă electronică ceea ce trebuie observat este că toate aceste protocoale au propriile lor chichițe, legate fie de specificații, implementare sau operare. O echipă roșie va încerca să puncteze problemele legate de elementele slabe de securitate privind integritatea, autenticitatea, confidențialitatea și disponibilitatea.

Abordând vulnerabilitățile din perspectiva tehnică a ceea ce ar putea să exploateze o echipă roșie, poate fi făcută clasificarea următoare.

Colectarea informațiilor despre structura rețelei țintă, sistemelor și utilizatorilor care o exploatează, este un punct de start bun. Aproape toate informațiile care pot fi obținute pot fi folositoare fie direct fie indirect într-o situație viitoare. Această informație, chiar fără sens la prima vedere, poate ajuta la identificarea punctelor slabe. Informațiile din această categorie sunt clasa și tipul sistemului de operare și clasa și tipul de servicii oferite. Lăsând deoparte serviciile directoare pentru utilizatori publici, care conțin o informație bogată, în unele cazuri sunt incluse adresele personale de acasă și numerele de telefoane.

Exemplu: O modalitate de obținere a unei vederi de ansamblu privind serviciile oferite de un server este determinarea tipului de servicii care sunt oferite (ascultate) pentru conexiunile la acel server. Într-un mediu bazat pe TCP/IP utilizarea normală a bine-cunoscutelor servicii este limitată la numerele de port TCP/IP stabilite exact. De exemplu serviciile FTP sunt oferite pe portul 21, e-mail (SMTP) pe portul 25 și www pe portul 80. Prin trimiterea cererilor de conectare la toate numerele de port și înregistrarea răspunsurilor obținute este ușor să spună ce servicii sunt ascultate (acceptate) și astfel oferite.

Această tehnică populară este cunoscută sub denumirea de *scanarea porturilor.* O dată ce toate informațiile sunt colectate, poate fi făcută o căutare pentru vulnerabilitățile cunoscute care se potrivesc sistemului de operare detectat, serviciilor și versiunii.

O tehnică foarte cunoscută pentru a crește (a spori) un privilegiu este exploatarea unei legături de încredere între două părți de încredere. O implementare bine-cunoscută a acestei tehnici este numită *spoofing* (imitație). Cele mai multe protocoale și servicii au deficiențe privind mecanismele bune de identificare a părții care expediază pachete. Tehnica *spoofing* utilizează aceste prescurtări pentru a falsifica sursa unui pachet. Când partea receptoare primește acest pachet falsificat el presupune că este în comunicație cu gazda de încredere adevărată când de fapt el are de-a face cu atacatorul.

Altă metoda de a exploata o legătură de încredere este forțarea *(hijacking)* unei conexiuni existente între două părți de încredere. Fără măsuri adecvate, numai stabilirea conexiunii este autentificată. Modalitatea cea mai răspândită pentru autentificare este prin tipărirea unui nume utilizator și a unei parole. Odată ce sesiunea este stabilită este posibil să se intre în sesiune fără să mai fie nevoie de re-autentificare. Evident această tehnică este numită forțarea conexiunii *(conection hijacking)*.

Exemple concrete ale exploatării legăturii de încredere este modul cum programele utilitare pot conduce la erori. Echipa de Răspuns de Urgență pentru Calculatoare (CERT) avertizează despre acest tip de atac în sfaturi CERT 95-01.

„Ușa din spate reprezintă un nume al familiei de programe de tipul Cal Troian care deschid noi vulnerabilități de securitate pentru sistemele pe care sunt executate". O ușă din spate poate fi introdusă fie pe timpul fazei de dezvoltare de către programator, sau într-un stadiu ulterior de către atacator. Prezența și aplicațiile ușilor din spate pot fi foarte puternice. O echipă roșie poate utiliza ușile din spate documentate/cunoscute sau poate să introducă propriile uși.

Un exemplu pentru mediile Unix este RootKit. Acesta constă dintr-un set de unelte de modificare sistem (ex. login) echipat cu uși prin spate. O dată ce un hacker a obținut controlul asupra sistemului de operare Unix, el înlocuiește uneltele sistem adevărate cu cele din RootKit. Uneltele sistem modificate oferă posibilitatea de a obține accesul în sistem prin utilizarea ușilor din spate instalate.

În mediile Microsoft Windows un exemplu popular este programul hacker „Back Orifice". Esența exploatării constă în faptul că programul de tip Cal Troian trebuie să fie instalat și activat pe sistemul țintă de câteva ori. Modul uzual de a realiza asta este prin trimiterea unei anexe e-mail pentru utilizatorul țintă ignorant. Prin ascunderea Calului Troian într-un mic joc, imagine sau felicitare, acesta se va activa când utilizatorul țintă deschide

mesajul. O dată instalat, controlul complet asupra țintei este garantat, prin conectarea la distanță utilizând mouse-ul și tastatura. O demonstrație a acestui atac face utilizatorii să fie informați despre riscurile care sunt introduse prin executarea anexelor e-mail neverificate.

Termenul de interzicere a serviciului sună malițios și într-un anumit fel așa și este. Totuși atacurile controlate de interzicere a serviciului pot fi de folos pentru alte atacuri, de exemplu exploatarea legăturii de încredere explicată mai înainte. Atacurile de interzicere a serviciului pot exista pe multe straturi. Un exemplu dat aici se referă la protocolul care este utilizat în cadrul Internet numit TCP/IP. O parte a protocolului este orientat pe conexiune Protocolul de Control al Transmisiei (TCP). Unul dintre cele mai bine cunoscute exemple de interzicere a serviciului cu TCP este numit inundare sincronă *(SYN-flooding)*. În continuare vom intra în unele detalii tehnice.

Stabilirea unei sesiuni TCP constă dintr-un proces numit strângere de mână pe trei căi *(three-way handshake)*. Acest proces este reprezentat în figura 1.

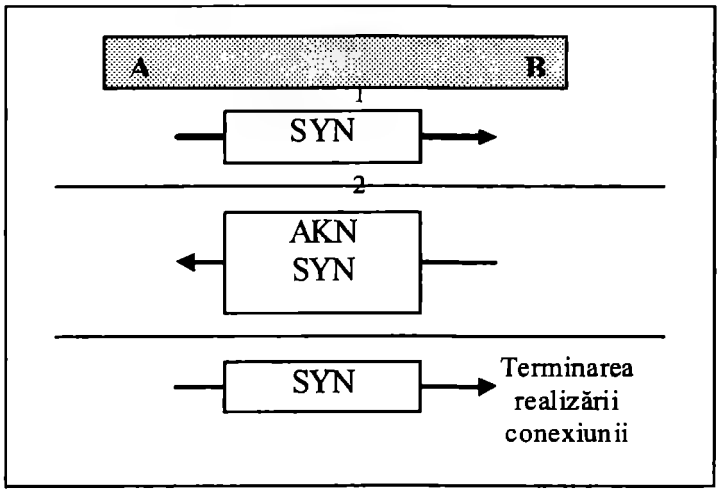


Figura 1: TCP/IP strângere de mână pe trei căi

Ne imaginăm că un client A vrea să stabilească o conexiune cu serverul B. Pentru a începe conexiunea clientul va trimite un pachet ce indică dorința lui de a stabili (sincroniza) o conexiune (SYN). Serverul B va confirma că a recepționat acest pachet prin trimiterea unui pachet de confirmare (luare la cunoștință) (SYN+ACK).

În această etapă conexiunea este pe jumătate deschisă. Pentru a încheia strângerea de mână pe trei căi clientul A va emite un semnal că a luat la cunoștință despre pachetul recepționat de la serverul B (ACK). În acest moment clientul A poate să schimbe date cu serverul B.

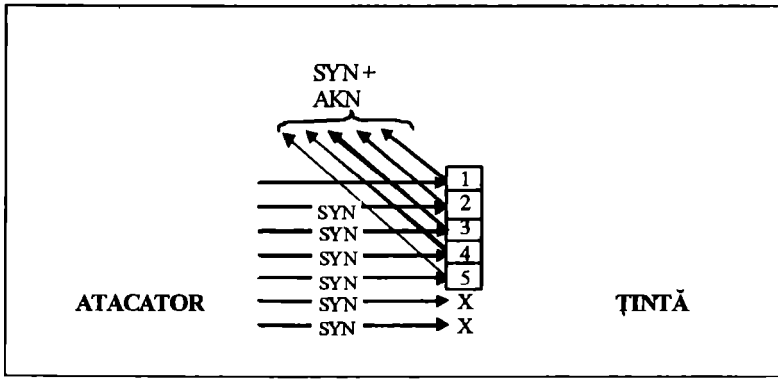


Figura 2. Exemplu de interzicere a serviciului: inundare SYN

Una dintre problemele cu setarea de mai sus este numărul limitat de sesiuni care pot fi în stare de deschis pe jumătate pe serverul B. Acest număr de sesiuni este numit *backlog* (conectări în fundal) și depinde de tipul sistemului de operare, dar în mod normal va fi în jur de 4-6 sesiuni. Dacă clientul nu ia cunoștință de pachetele trimise de server, serverul va trata această sesiune că a depășit timpul *(time-out),* va reîncerca restabilirea de câteva ori și în final va șterge detaliile din *backlog.*

Durata totală a acestui proces fi de 10 minute. Acum să ne imaginam scenariul descris în figura 2.

În combinare cu tehnica de spoofing explicată mai devreme, atacatorul va forța un număr de solicitări de stabilire a conexiunii (destul ca să umple *backlog-ul* serverului). Ținta crede că, comunică cu o gazdă, alta decât atacatorul. Această gazdă nu este capabilă totuși să răspundă (fie este prea ocupată fie este inexistentă). În acest moment ținta nu va accepta noi conexiuni *(backlog-ul* lui este plin oricum) și va aștepta până când fie primește luările la cunoștință pentru conexiuni sau ajunge la depășire de timp.

Această tehnică numită *SYN-flooding* reprezintă o interzicere a serviciului foarte eficientă. Atacatorul are nevoie să trimită câteva pachete false la fiecare 5 sau 10 minute pentru a realiza scoaterea efectivă din funcțiune a țintei. Acest tip de atac este puțin utilizat astăzi, dar cu doi ani în urmă el reprezenta o vulnerabilitate exploatată frecvent. Atacul pasiv este un atac fără ca ținta să-și dea seama că este supusă unui atac. Un exemplu de atac pasiv este posibilitatea de a citi toate pachetele de pe firele de conexiune, tehnică cunoscută sub denumirea de *sniffing* (strănut) sau *snooping* (sughiț). Pe timpul operării normale o placă de interfață la rețea (NIC) prelucrează numai pachetele destinate plăcii proprii și le trimite la nivele superioare. Prin punerea plăcii într-un mod special (mod dubios) toate pachetele care ajung la NIC vor fi prelucrate. Utilizarea legitimă a acestei caracteristici ar trebui administrată în rețea și corectată.

Totuși, posibila utilizare greșită a acestei caracteristici este mult mai profundă. Programe specializate se găsesc pe Internet și identifică sesiunile de autentificare necriptate (care pot include parole) sau alte date senzitive. În general tot traficul necriptat este marcat, acesta include e-mail și sesiuni Web. O echipă roșie poate utiliza această tehnică pentru o diversitate de motive. Uneori informația culeasă scoate în evidență că ținta lucrează cu materiale senzitive sau secrete, într-o manieră neadecvată sau într-o rețea nesecretă. În alte cazuri informația poate fi utilizată pentru a lansa noi atacuri asupra sistemelor sau pentru a extrage parole pentru accesul neautorizat la sistemele țintă.

Majoritatea atacurilor pot fi plasate în această categorie. Cele mai multe pachete software comerciale de scanare a vulnerabilităților cum ar fi *Internet Security Scanner* (IIS) și *Network Associates CyberCop* identifică găurile în software sau într-un sistem de operare. Din cauza diversității lor nu poate fi dată o descriere generală. Un bun exemplu ce explică impactul posibil este dat mai jos.

Serviciile cele mai uzuale cu care oamenii se ocupă în prezent sunt prezentate la nivel aplicație. Servicii ca poșta electronică (SMTP), protocolul de transfer al fișierelor (FTP), și WWW (HTTP) sunt cele mai cunoscute. Una din vulnerabilitățile de implementare a acestor protocoale este numită în mod curent depășirea de memorie *(buffer overflow).*

Depășirea de memorie apare când se plasează un obiect de o anumită dimensiune într-o zonă de memorie prea mică rezervată în acest scop. Un exemplu practic este procesul de conectare *(login)* utilizând parole. În mod normal o parolă nu va depăși un număr de 16 caractere. Ce se va întâmpla dacă sunt inserate 300 sau chiar mai multe caractere la dialogul de interogare a parolei? O interpretare grafică este descrisă în figura 3.

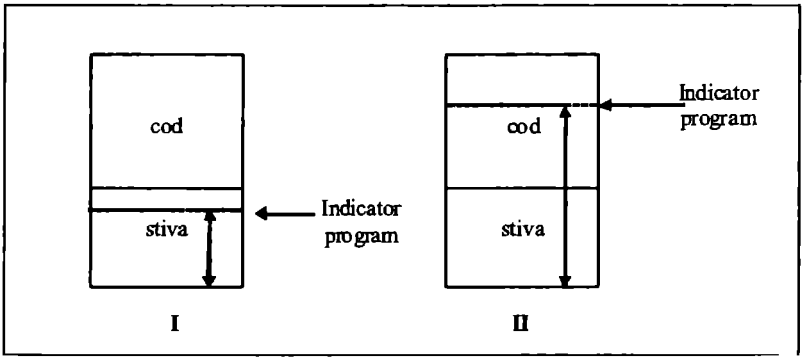


Figura 3: Principiile care stau în spatele depășirii de memorie (overflow).

Situația normală (simplificată) este reprezentată în situația I. Poziția actuală a rulării programului sursă este păstrată de un contor numit contor de program. Valorile de intrare sunt stocate în stivă, care este dinamică. Programul va citi informația de intrare, o va pune în stivă (ex. parola) și o va șterge după ce termină utilizarea ei.

Când nu sunt făcute verificari de limite aceste valori de intrare pot, dacă depașesc zona de memorie alocată, să suprascrie alte părți de program, incluzând codul program (vezi situația II). Comportamentul normal când au loc depășirile de memorie se manifestă printr-o interzicere a serviciului. Totuși dacă datele de intrare sunt puse într-un mod special cineva poate să suprascrie codul program cu noi instrucțiuni program.

Efectul tuturor acestora ar fi că de exemplu procesul de autentificare (în cazul exemplului cu parola) execută cod arbitrar introdus de atacator. Acest cod va rula în contextul de securitate al procesului în chestiune, procesul de autentificare. Dacă contextul de securitate este destul de înalt, poate fi obținut întregul control al sistemului de operare.

Pentru punerea acestei teorii în practică un atacator are nevoie să cunoască poziția precisă (deplasamentul) pentru codul care trebuie inserat. Cu toate vulnerabilitățile, o dată ce oamenii găsesc una dintre ele, sunt realizate pentru utilizare publică scripturi și unelte automate la scurt timp după anunțarea acesteia. Cele mai multe depășiri de buffer exploatează codul de protecție inserat din care va răsări o rădăcina de protecție ce va da controlul total atacatorului.

Când sunt primite sfaturile de securitate de la Echipa de Răspuns de Urgență pentru Calculatoare (CERT) și Recomandări pentru Incidente Calculator (CIAC) pot fi găsite avertizări pentru aceste vulnerabilități de depășire a memoriei. Un exemplu este recomandarea CERT 07 (16 iunie 1999). Având un zid de foc activat, dacă este configurat și menținut corect, el poate preveni multe atacuri. Dar ce se întâmplă dacă utilizatorii folosesc stații

de lucru echipate cu modem-uri pentru a realiza propria lor conexiune la Internet sau la alte rețele. Zidul de foc *(firewall)* al corporației va fi de eficiență redusă. O modalitate pentru echipele roșii să identifice acestea și sistemele corespunzătoare este utilizarea echipamentului pentru scanarea domeniului telefonic pentru modem-urile active.

În unele cazuri modem-urile găsite sunt instalate de către administratorii de rețea pentru a facilita managementul de la distanță. O idee nobilă dar mortală, dacă este utilizată de către altcineva. Pe lângă vulnerabilitățile tehnice, o mulțime de erori rezultă din lipsa unei (bune) politici de securitate și a măsurilor organizaționale, care includ proceduri pentru managementul operațional, managementul de schimb, politica utilizată pentru acceptare etc.

În practică, echipele roșii găsesc adesea în lucru versiuni ale sistemelor de operare sau ale serviciilor care au vulnerabilități cunoscute. Deși sunt disponibile actualizări, petece sau corectări oferite de vânzător, administratorii aleg să nu instaleze aceste corectări dintr-o varietate de motive. Consecințele pot să fie dezastruoase.

Exploatarea unei vulnerabilități cunoscute într-un sistem identificat ia mai puțin de o secundă pentru a distruge zile sau săptămâni de muncă. Datorită creșterii interconectivității, răspândirea informației referitoare la vulnerabilități este foarte rapidă. Când cineva din SUA găsește o vulnerabilitate și publică detalii despre ea, unelte pentru exploatarea ei vor apărea la scurt timp după acesta și sistemele de la alt capăt al lumii vor fi atacate în aceeași zi. Administratorii nu au altă variantă decât acționarea fermă și mulțumirea cu securitatea informațiilor oferită de vânzătorii lor și/sau echipele CERT când este posibil.

În alte cazuri securitatea funcțiilor este implementată dar nu este pusă în funcțiune. Administratorii sunt mai mult decât fericiți dacă au reușit să instaleze pachetele software cu succes, iar ultimul lucru în mintea lor este să depună efort pentru activarea

elementelor de securitate. Aceasta se reflectă în istoria și modul de desfășurare al proceselor, prin punerea accentului pentru proiectarea rețelei și a sistemelor mai mult pe funcționalitatea dorită și pe ușurința utilizării. Cerințele de securitate sunt (cu noroc) pe locul doi în această proiectare. Așa cum s-a menționat înainte, tehnologia anilor 1970 (TCP/IP) pe care Internetul se bazează, nu are măsuri standard pentru oferirea de confidențialitate, autenticitate și integritate.

Și chiar dacă funcțiile de securitate sunt implementate, puterea unui sistem se reflectă în legăturile sale slabe. O situație cu care echipele roșii se întâlnesc frecvent este utilizarea de parole slabe sau a nici unei parole pe durata procesului de identificare și autentificare, care te face să te întrebi de ce acest element de „securitate" a fost instalat pe primul loc.

Dar chiar parole dificile sunt sparte în timp de ore sau chiar minute. Principiul din spatele celor mai mulți spărgători de parole, nu este posibilitatea decriptării parolelor, ci compararea parolei criptate cu rezultatul criptat al unui set de caractere de intrare utilizat. Spărgătorii de parole utilizează astfel două abordări.

Atacul dicționarului. Prin criptarea cuvintelor dintr-un dicționar și compararea rezultatului cu parola criptată. Dacă parola aleasă este listată într-un dicționar este o problemă de minute înainte ca parola să fie găsită. Cineva ar fi surprins să vadă cum mulți oameni utilizează cuvinte uzuale sau nume ale activităților lor. Cum ar fi „bună încercare dar nu merge". Cei mai mulți spărgători de parole verifică automat diferite variante ale dicționarului prin adăugarea de cifre sau prin despărțirea în silabe.

Forța brută. Toate combinațiile de caractere posibile sunt criptate și comparate cu parola criptată și care vor conduce eventual la parola căutată. Deoarece programul popular de spargere de parole pentru Microsoft Windows NT declară: *„Toate parolele alfanumerice pot fi găsite într-un interval mai mic de 24 de ore pe un Pentium II/450".*

Pe lângă mijloacele tehnice de obținere a informațiilor, modalitatea tradițională de obținere a informației poate fi la fel

de fructuoasă. Când se face un test de pătrundere în interior, o observare fizică a camerelor unde sunt situate țintele poate fi o posibilitate. Un fapt de viață este că oamenii tind să scrie lucrurile pe care au nevoie să și le reamintească.

Altfel spus, nume de login, parole, nume de sistem și chiar informații personale cum ar fi numerele cărților de credit și numerele de securitate socială sunt scrise și stocate într-un loc accesibil membrilor echipei roșii. Informația obținută poate ajuta de asemenea la ghicirea căii de urmat pentru intrarea în sistem. De multe ori sunt utilizate numele comune sau numele legăturilor lor ca bază pentru parole. Această tehnică numită *ghicirea de parole, reprezintă* noroc chior.

Pe lângă informația stocată pentru reutilizare, de asemenea lucrurile aruncate după caz la coșul de gunoi pot fi folositoare. Există chiar un nume asociat acestei tehnici care este *trashing* (recuperare).

Un nivel adesea uitat, dar cu toate astea foarte puternic, este nivelul mental. Acest nivel se referă la mijloace psihologice de influențare a oamenilor. O tehnică angajată de unii hackeri este *ingineria socială.*

Imaginați-vă comportamentul utilizatorilor unei rețele a corporației când cineva sună spunându-i că el este administratorul rețelei: *„Domnule, noi avem o problemă cu utilizatorii bazei noastre de date, unele înregistrări au fost șterse din greșeală. Puteți să-mi spuneți parola dvs. așa încât să pot să repar înregistrările"*. Ați fi surprins să vedeți câți oameni sunt gata să ajute dându-și parola. Sau ce se întâmplă când oamenii din departamentul de management al sistemului primesc o scrisoare de la vânzătorul echipamentelor lor, care le spune că este nevoie neapărat să instaleze programul de corectare *(patch)* inclus. Când este instalat „patch-ul" va introduce o ușă prin spate pentru atacator. Aceasta va lucra garantat dacă departamentul de management al sistemului va primi scrisoarea cu câteva zile înainte de Craciun.

Destul de impresionant este că multe echipe roșii nu utilizează în prezent aceste tehnici, care dacă sunt utilizate într-o manieră

corectă pot fi foarte utile vizavi de programatori sau de educarea utilizatorilor.

Prevenirea exploatării vulnerabilităților sociale este chiar dificilă. Parte a acesteia trebuie să fie realizată prin politici utilizator acceptabile și educarea utilizatorilor. Pe de altă parte, pentru menținerea nivelului de securitate există o mare preocupare pentru ceea ce se spune și comportamentul asociat al utilizatorilor.

Fiecare efort de analiză este diferit de alt efort și nu este posibil să fie realizată o „carte de bucate" pentru abordarea unei echipe roșii. Totuși, este posibil să se ofere o vedere de ansamblu a modului cum un astfel de grup își face treaba. Procesul descris aici este aplicabil sistemelor ce au conexiuni de rețea externe (ex. Internet). Pentru sistemele ce au conectivitate externă, o parte a tuturor analizelor de vulnerabilitate poate fi realizată dintr-o locație de la distanță.

Efortul unei echipe roșii începe de obicei cu o cerere sau sugestie ca un anume sistem să fie subiectul unei analize. Odată ce autoritățile abilitate sunt de acord cu activitatea de analiză, echipa roșie începe să colecteze orice informație disponibilă despre structura sistemului analizat. Înainte de a face asta trebuie îndeplinite posibilele aspecte legale.

Aceasta necesită ca echipa roșie să aibă o clară înțelegere a limitelor rețelei din „cyberspațiu" care urmează să fie analizate. Aspectele legale ar trebui să fie bine înțelese și cunoscute dinainte. Ar trebui considerate de asemenea riscurile de accesare neintenționată a rețelelor din afara limitei intenționate.

De exemplu, când o evaluare este făcută pentru vulnerabilitățile rețelelor din Olanda, legea infracțiunii prin calculator, Directiva Europeană pentru Intimitate Privată și legea telecomunicației restricționează echipele roșii în „libertatea" lor de a opera. Evident proprietarul rețelei analizate ar trebui să-și asume responsabilitatea dată de abordarea profesională și limite legale ale echipei roșii. După ce toate aceste aspecte au fost asumate, echipa roșie poate să înceapă treaba.

Mai întâi, tipologia fizică a rețelei este detaliată - dacă rețeaua utilizează cablu coaxial, cablu cu două fire, sau fibră Ethernet; locația, modelul și tipul de router-e, bridge-uri și hub-uri. Pe urmă este topologia logică a rețelei - locația serverelor cheie (ex. DNS, Web); spațiul de adrese de IP și orice subrețea ce este implementată. Frecvent, este de mare ajutor realizarea unei diagrame sau desenarea componentelor cheie ale sistemului de analizat.

Atât vederile de ansamblu cât și de detaliu sunt folositoare, dar invariabil devine necesară producerea unei singure diagrame ce arată toate componentele semnificative pe o singură pagină, fără să depindă cât de mare sau cât de mică este acea pagină pentru ca toate componentele să fie lizibile. Pe cât posibil, e nevoie ca această informație să fie colectată înainte de etapa activă a analizelor de vulnerabilitate. Este o muncă dificilă, dar înțelegerea întregului sistem aflat în analiză este crucială pentru succesul întregului efort.

Având colectată în avans cât mai multă informație, echipa roșie trece la faza vizibilă de analiză pe site. Aici este locul unde sunt aduse unelte de analiză de vulnerabilitate, *sniffere*, unelte de mapare (întocmire hărți), pachete de desenare și alte unelte de reprezentare documentată a sistemului așa cum este el implementat. Pe cât este de important să existe suport local și coordonare pentru această fază a analizei, pe atât este, de asemenea, important să se evite transformarea vizitei site-lui într-un eveniment special, făcând imposibilă obținerea unei viziuni imparțiale a operării normale a sistemului.

Deoarece surprizele nu sunt plăcute pentru nimeni, este important să se limiteze cunoașterea dinainte a vizitei echipei roșii la un număr de câteva persoane. Pentru a evita conflictele, personalul local cunoscător trebuie să fie disponibil pentru a trata orice preocupări sau furnizări greșite din partea responsabililor care nu au fost informați cu privire la efortul de analiză.

În general, o echipă roșie va avea sisteme portabile încărcate cu pachetele software necesare pentru realizarea analizelor de

vulnerabilitate - uneltele menționate mai sus. Echipele roșii ar trebui echipate, de asemenea, cu o mare varietate de componente de rețea pentru a facilita accesul la sistemele aflate în analiză.

Cabluri, hub-uri rețea, testere de cablu, prize triple de alimentare, conectoare, adaptoare, multimetre, role de cablu, unelte de prindere, unelte de lipit, unelte de mână, o imprimantă portabilă și multe altele vor fi toate utile la un anumit moment dat. În timp, fiecare echipă va colecta setul de unelte de care are nevoie, dar este întotdeauna mai bine pentru o echipă roșie să fie dotată complet, decât să implice personalul al cărui sistem este analizat.

Membrii echipei vor pierde de obicei câtva timp să verifice informația culeasă înainte și să colecteze orice altă informație care lipsește din datele inițiale. În particular, este importantă verificarea dacă topologia actuală a unui sistem se potrivește cu documentația. Semnalarea discrepanțelor minore poate schimba semnificativ rezultatele de ansamblu.

De exemplu, o conexiune rețea furnizată pentru posibilitatea configurării de la distanță când un sistem este prima dată instalat, poate fi uitată și lăsată acolo până când sistemul este complet pus în funcțiune. Verificarea setului documentat de servicii de informații este, de asemenea, important, deoarece fiecare serviciu de informații aduce propriul set de vulnerabilități pentru serverele și clienții implicați. O dată ce topologia sistemului și informația a fost verificată, echipa poate identifica elementele cheie (ex. servere primare, clienți obișnuiți, elemente rețea cheie) pentru analize de vulnerabilitate detaliate.

După ce vulnerabilitățile au fost identificate, echipa roșie începe procesul de elaborare a unui raport pentru autoritatea care a autorizat analiza. Există trei aspecte cheie a modului în care această fază a procesului decurge. Mai întâi, **raportul de analiză trebuie să fie complet și accesibil**.

Raportul este de mică valoare dacă nu explică vulnerabilitățile și nu sugerează remediile într-o manieră care poate fi înțeleasă și apoi pe baza lui acționat de către personalul responsabil pentru

sistemul subiect. Unele dintre uneltele angajate într-un efort de analiză generează documentație ca parte a operării lor; combinând ieșirile acestor unelte cu alte informații (ex. diagramele de topologie a rețelei) pentru a produce un raport succint și complet este o altă parte a activității echipei roșii.

În al doilea rând, **nimănui, dar nimănui, nu-i place să fie apostrofat**. Pentru a pune asta în context, este esențial ca rezultatele unui efort de analiză să fie discutate cu personalul afectat de aceste rezultate, cu participarea sau contribuția autorității de autorizare, înainte ca rezultatele să fie prezentate în întregime structurii de management/comandă implicate. Aceasta permite personalului afectat să înțeleagă rezultatele și implicațiile fără să fie pus în situația de apărare și să crească probabilitatea de recepție pozitivă a rezultatelor.

În final, echipa roșie trebuie să-și amintească faptul că **rezultatele analizelor aparțin autorității autorizate**. Rezultatele analizelor de topologie a rețelei, datele de vulnerabilitate colectate și raportul însuși sunt informații privilegiate și nu ar trebui să fie oferite altora fără permisiunea expresă în primul rând a entității care a autorizat analiza. De fapt, este uzual pentru echipele roșii să utilizeze calculatoare notebook, cu drivere de disc înlocuibile astfel încât echipele pot lăsa toate datele reziduale autorității de autorizare.

Din nou, deoarece aceasta nu este o descriere completă a tuturor considerațiilor și activităților ce au loc pe timpul unei analize a echipei roșii, ea oferă unele incursiuni în operațiile unei astfel de activități. Pentru a înțelege echipa roșie mai complet, este probabil cel mai bine să fie realizate pentru câtva timp unele analize de vulnerabilitate de laborator, și apoi să se treacă la activități de teren.

În timp, fiecare echipă găsește combinațiile de unelte, tehnici și personal ce se potrivesc cel mai bine sistemelor pe care ei le analizează. Frecvent, unelte similare multiple vor fi utilizate separat sau în combinație. De exemplu personalul echipei roșii a Agenției NATO C3 (NC3A) utilizează de obicei două tipuri de

analiză LAN diferite (ex. sniffers), ținând cont pe de-o parte de posibilitățile diferite ale celor două produse și pe de altă parte de preferințele individuale ale membrilor echipei.

Membri diferiți din echipă vor aplica tehnici diferite pentru obținerea aceleiași informații. Cineva adept al sistemului Unix va selecta probabil utilizarea programului *snoop* mai curând decât o analiză de LAN externă.

Un grup va prefera scanarea de vulnerabilități pentru ISS, pe când altul utilizează CyberCop și un alt grup va lucra cu ambele unelte. Familiarizarea cu un număr mare de unelte și câteva implementări ale fiecărui tip de unealtă este mai importantă decât selectarea „celei mai bune unelte". Și „trusa de unelte" a echipei se va schimba în timp.

Dezvoltarea unei metode de lucru a echipei este probabil mai importantă decât selecția uneltelor. Personalul va avea nevoie să petreacă câtva timp să lucreze cu uneltele proprii în laborator pentru a se familiariza ei înșiși cu operarea și interpretarea corectă a rezultatelor. Ei trebuie, de asemenea, să petreacă ceva timp pentru a lucra unul cu altul, să vadă care e modul de lucru al fiecărui membru al echipei și care sunt punctele lui slabe și tari. Acest aspect s-a dovedit a fi crucial, deoarece membrii capabili ai echipei obișnuiau frecvent să aibă o contribuție de leader în activitățile profesionale anterioare.

Echipele roșii trebuie de asemenea să dezvolte o metodă de lucru cu personalul responsabil de sistemele pe care echipa le va analiza. Aici este foarte important să se mențină legături de cooperare și nu de adversitate.

Echipele roșii vor fi angajate frecvent ca un pas în procesul de acreditare a sistemelor operaționale precum și pentru revizuirea posturii de securitate a sistemelor existente. În ambele cazuri, este important să existe o coordonare apropiată cu operatorii sistemului, o aprobare din partea structurii lor de management/comandă. Este de asemenea important să fie utilizați cel puțin doi sau trei analiști în fiecare efort, atât pentru a împărți munca cât și pentru a furniza

„două pereche de ochi" pentru problemele importante. Când este posibil, este de asemenea de ajutor să fie desemnat un membru special al echipei care să se ocupe de orice problemă apărută între echipa roșie și personalul operațional local.

Aspectele cheie menționate în secțiunea precedentă despre activitățile echipei roșii și aplicabilitatea lor, au pierdut din vedere un aspect minor dar nu l-au uitat - costurile formării și menținerii unei echipe roșii. Pe scurt aceste costuri sunt substanțiale. Cum s-a menționat mai înainte este nevoie de unelte și software specializate, lăsând deoparte disponibilitatea unor profesioniști de încredere cu performanțe și cu o instruire ridicată.

Suplimentar procesul complet de culegere de informații, analiza pe site și raportarea rezultatelor în timp. Efortul final trebuie făcut pentru optimizarea procesului în derulare, specific metodelor și tehnicilor echipei roșii pentru a asigura că acele cunoștințe imediate despre noile dezvoltări și tehnologii devin disponibile.

O echipă roșie joacă un rol modest până la unul efectiv în tabloul mai mare al domeniilor securității și siguranței informaționale. Totuși, tipurile de vulnerabilități care pot fi găsite pe timpul activităților echipei roșii sunt de folos în procesul de dezvoltare și de menținere a bazelor securității informației - politica de securitate. Politica de securitate descrie procedurile organizaționale și măsurile tehnice pentru a reduce și elimina riscurile.

Fără o astfel de politică, un incident întâmplător poate duce la o pierdere financiară considerabilă. O echipă roșie va oferi o parte a soluției prin identificarea și raportarea punctelor slabe într-o infrastructură de tehnologia informației concretizată prin luarea de măsuri adecvate. La final este mai bine să previi și să stai departe de necaz în loc să aștepți ca lucrurile să se întâmple.

OPERAȚIILE INFORMAȚIONALE UN MIJLOC DE DESCURAJARE STRATEGICĂ

ANCA MONICA POPA

Mediul informațional actual devine tot mai complex, dezvoltarea tehnologiilor informaționale revoluționând modul în care națiunile, armatele, organizațiile și oamenii interacționează. Fuziunea rețelelor de informații, a bazelor de date și a tehnologiilor aduc informația foarte aproape de fiecare. Avantajul informațional presupune cunoașterea foarte bună a ceea ce înseamnă informație și abilitatea de a lucra cu o colecție de informații, de a o procesa, utiliza și disemina în locul, la momentul și pentru scopul potrivit.

Exploatarea avantajelor oferite de puterea tehnologiilor informaționale, alături de o recunoaștere a potențialului informației, se reflectă în ceea ce este numită operație informațională.

Aplicarea de operații informaționale (O.I.) în cadrul coalițiilor în timp de pace, înseamnă adaptarea strategiilor de război la starea de pace, integrarea funcțiilor **O.I.** într-un mediu multinațional fiind o adevărată provocare.

In ultimii ani, în unele state membre N.A.T.O., operațiile informaționale au devenit un concept doctrinar dezvoltat. Deși nu este acceptat în întregime de alte țări, acesta reflectă nevoia de a surprinde aspectele unui fenomen care merge dincolo de conceptele tradiționale de război.

O.I. este o strategie integrată care răspunde la noi vulnerabilități și creează, în același timp, noi oportunități. El introduce în discuție acele elemente nemilitare ale puterii, cum ar fi: politicile, relațiile internaționale, finanțele, infrastructura, percepția publică etc.

REPERE CONCEPTUALE

Nu există o definiție universal acceptată care să acopere întreg conținutul conceptului de O.I.

Politica N.A.T.O. referitoare la O.I. afirmă: *„Operațiile informaționale sunt acțiuni întreprinse pentru a influența factorii de decizie, în conformitate cu anumite obiective politice și militare, prin afectarea informației și a proceselor care se bazează pe informație"*[64].

In cuprinsul documentului se precizează că: *„Operațiile informaționale integrează războiul de comandă și control cu procesul de consultare politicii, cu aparatul de luare a deciziei și cu operațiile politico-militare ale Alianței (...)"*. De asemenea, (...) *schimbarea operațională importantă constă în concentrarea pe rolul informației. Acest lucru include aspectele de percepție, ca și pe cele tehnice. Planificarea militară nu necesită numai implicare directă a aparatului politic de luare a deciziei, dar și o implicare și o integrare mai largă a unor elemente din conducerea militară"*.

In context multinațional, dar la nivelul trupelor de uscat"[65], americanii definesc operațiile informaționale ca fiind: *operații militare permanente în cadrul mediului informațional care dau posibilitatea, întăresc și protejează abilitatea forței aliate de a culege, procesa și utiliza informația pentru a obține avantaj față de toate categoriile de operații militare"*. Se mai afirmă că acestea presupun *„exploatarea capacităților de informare și decizie ale adversarului sau chiar sabotarea acestuia în procesul de luare a deciziilor, prin împiedicarea accesului său la informații"*.

O definiție americană mai recentă, figurând în „Doctrina integrată a operațiilor informaționale"[66] arată că acestea *„reprezintă acțiuni desfășurate în scopul afectării informațiilor și sistemelor*

---

[64] Citat extras din documentul Comitetului militar MC-422, 15 decembrie 1998, aprobat de Consiliul Nord Atlantic pe 22 ianuarie 1999

[65] In documentul FM 100-6 „Information Operations", 27 aug. 1996

[66] „Joint Doctrine for Information Operations", *Joint Pub.*3-13, 9 oct. 1998

informaționale ale adversarului, concomitent cu protejarea propriilor informații și sisteme informaționale". Lectura documentului permite constatarea că aceste operații necesită integrarea strânsă și continuă a capacităților și acțiunilor ofensive și defensive, precum și o proiectare, integrare și interacțiune eficientă a sistemelor de comandă-control, cu sprijinul asigurat de activitatea de informații.

Strategii ruși susțin că operațiile informaționale sunt *„o cale de rezolvare a unui conflict dintre două părți. Scopul este că una dintre părți să câștige și să păstreze avantajul informațional asupra celeilalte. Acest lucru poate fi realizat prin exercitarea unei influențe informaționale/psihologice și tehnice specifice, prin sistemele naționale de luare a deciziei prin intermediul populației, prin structurile sale informaționale, ca și prin înfrângerea sistemului de control al dușmanului, a structurilor sale informaționale cu ajutorul unor mijloace suplimentare, precum armele, materialele nucleare"*[67].

Reflectând asupra acestor definiții trebuie subliniat faptul că, deși diferă, au totuși și unele elemente comune.

In primul rând, trebuie avută în vedere informația. Informația se aseamănă mai degrabă unui bun.

Informația, ca dimensiune centrală a competiției și a conflictului, ar trebui să ocupe *„linia întâi"* în organizarea arhitecturii sistemului național de apărare și ar trebui să devină, în percepția liderilor politico-militari, o dimensiune egală, cel puțin, cu cea terestră, aeriană și maritimă.

In al doilea rând, trebuie să ne referim la sistemele (structurile) informaționale, prin care se înțelege totalitatea infrastructurilor, organizațiilor, personalului și componentelor care realizează culegerea, prelucrarea, stocarea, transmiterea, afișarea și diseminarea informațiilor, precum și acțiunile care au loc ca urmare a informațiilor obținute. De reținut că sistemele informaționale includ și procesele orientate către informații.

---

[67] „A Russian View of Future War: Theory and Direction", *The Journal of Slavic Military Studies,nr.3/1996*

În al treilea rând, trebuie luat în calcul conceptul de superioritate informațională. Prin acesta se înțelege *„capacitatea de a culege, procesa și disemina un flux continuu de informații, în timp ce este exploatată sau chiar interzisă abilitatea adversarului de a face același lucru".*

Nu în ultimul rând, trebuie vorbit despre factorii de decizie. In literatura de specialitate, acest concept de influențare a factorilor de decizie, direct sau indirect, mai poartă și numele de „război de percepție" sau „război neocortical".

DELIMITĂRI SI DIFERENTE

Înțelegerea locului și rolului actual al operațiilor informaționale, la orice nivel (politic, strategic, tactic etc.) și în tot spectrul de situații (pace, criză, conflict etc.), impune stabilirea unei distincții între acest concept și cele de *„război informațional"* și *„război de comandă-control".*

In sens strict militar, războiul informațional reprezintă *„operații informaționale desfășurate în perioade de criză sau de conflict, în scopul atingerii unor obiective sau influențării unor anumite ținte"*[68].

Războiul de comandă-control are, potrivit N.A.T.O.[69], următoarea înțelegere: *„Folosirea integrată a tuturor capacităților militare, inclusiv a operațiilor de securitate, inducerii în eroare, operațiilor psihologice, războiului electronic și distrugerii fizice, sprijinite de către sursele de intelligence și sistemele de comunicații și informatică, pentru interzicerea accesului la informație, influențarea, degradarea sau distrugerea capacității de comandă-control a unui adversar, în timp ce toate acestea sunt protejate împotriva unor acțiuni similare".* Cu alte cuvinte, războiul

[68] *„Report of Institute for Strategic Studies,* National Defense University, Washington, 1999

[69] Definit în documentul Comitetului militar MC-348, „Politica războiului de comandă-control", aprobat de Consiliul Nord-Atlantic în 1996.

de comandă-control înseamnă exact ceea ce afirmă și denumirea sa, executarea de acțiuni pentru prevenirea controlului adversarului asupra informației necesare, pentru realizarea de evaluări și decizii corecte.

Din formulările oficiale N.A.T.O. se desprinde mai greu diferența dintre conceptul mai vechi de război de comandă-control (1996) și cel de operații informaționale, recent adoptat (1999).

Cu toate că ambele se concentrează pe comandă-control, există o serie de elemente care le deosebesc.

Primul este legat de dependența crescândă a organizațiilor militare de tehnologia informațională și de comunicații. O mare parte din calitatea activităților de comandă-control depinde de calitatea datelor, de receptarea lor în timp util, de software-ul implementat în sisteme de tip C4I (Comandă, Control, Comunicații, Calculatoare, Informații) etc. Există acum noi mijloace de manipulare și de distrugere a acestor facilități. Așa cum este definit, războiul de comandă-control nu ia în calcul panoplia *„armelor informaționale"*[70]: software-ul malign (viruși, bombe logice, troieni, viermi), microcomponentele cu surprize, armele cu puls electromagnetic, microbii electronici (non-software) și, nu în ultimul rând, sistemele de suport decizional.

Al doilea element ar fi cel legat de faptul că operațiile informaționale nu se limitează doar la vremuri de criză sau conflict.

Un alt element este legat de conceptul de coordonare. Războiul de comandă-control necesită folosirea integrată a cinci acțiuni militare principale: războiul electronic, operațiile psihologice, inducerea în eroare, securitatea operațiilor și distrugerea fizică. Acești cinci piloni sunt discipline individuale, iar atunci când există coordonare și sprijin ferm din partea *intelligence-ului și* a comunicațiilor, întregul pe care ei îl produc - războiul de comandă-control - este mult mai mare decât suma tuturor părților.

---

[70] V. Păun, „Excurs în spațiul de conflict informațional", *Strategii XXI,* nr.2/1997, București.

Prin folosirea celor cinci piloni și a altor capacități militare într-o manieră coordonată, se obține o sinergie care permite acțiunea eficientă în cadrul unei crize/conflict.

Practic, războiul de comandă-control reprezintă aplicarea militară a operațiilor informaționale.

Operațiile informaționale nu înlocuiesc războiul de comandă-control, ci integrează această „strategie militară" în procesul de consultare politică, în aparatul de luare a deciziei și o combină cu operațiile politice și militare.

Noutatea constă în viteza și agilitatea operațiilor solicitate de era electronică, transparența mediului operațional, relativa „dispariție a distanței", natura tot mai efemeră a puterii etc. De asemenea, este nouă estomparea conceptelor „nivel strategic", „operațional" și „tactic". Viteza comunicațiilor, diminuarea rolului distanței și, în general, natura mult mai transparentă a mediului de conflict sunt împreună sursa acestei estompări. Mai mult, conceptele a ceea ce constituie „zona de operații", „zona de influență" și „zona de interes" ale comandantului își măresc semnificația datorită tehnologiei de calcul și lărgirii câmpului de luptă la ciberspațiu.

FORMELE DEFENSIVE ȘI OFENSIVE ALE OPERAȚIILOR INFORMAȚIONALE

Există două categorii principale de operații informaționale: operațiile informaționale defensive și operațiile informaționale ofensive.

Conform documentelor N.A.T.O., *„operațiile informaționale defensive integrează și coordonează politicile, procedurile, acțiunile, personalul și tehnologia, pentru protejarea și apărarea informațiilor și sistemelor informaționale"*[71] și conțin următoarele elemente:

• Siguranța informațională - protejează și apără informația

[71] Definiție figurând în documentul Comitetului Militar N.A.T.O. MC-422 *„Information Operation Policy"*, 22.01. 1999

prin asigurarea disponibilității, integrității, autenticității, confidențialității și imposibilității ignorării ei. Include măsurile necesare pentru restabilirea funcțiilor vitale ale sistemelor informaționale prin încorporarea unor capacități de protecție, detectare și reacție la atacuri. Utilizează tehnologii și proceduri de securitate la niveluri multiple, de control al accesului, de securizare a echipamentelor și de descoperire a acțiunilor cu caracter intrusiv.

• Securitatea informațională asigură protecția și apărarea sistemelor informaționale împotriva accesului neautorizat, a modificărilor conținutului informațiilor aflate în faza de stocare, prelucrare sau tranzit și împotriva interzicerii accesului utilizatorilor autorizați către aceste informații, înglobează, după standardul N.A.T.O., securitatea calculatoarelor (COMPUSEC) și securitatea comunicațiilor (COMSEC).

• Securitatea operațiilor - reprezintă procesul de identificare a informațiilor de importanță critică, de analizare a activităților proprii care pot fi observate de către sistemul informativ al (in)amicului, a indicațiilor pe care acest sistem le-ar putea obține, corela și interpreta, pentru a obține informații de importanță critică. Totodată, reprezintă procesul de alegere și executare a acelor măsuri care să elimine sau să reducă, la un nivel acceptabil, vulnerabilitățile în fața acțiunilor (in)amicilor.

• Contrainducerea în eroare - sprijină acțiunile defensive prin eliminarea, neutralizarea sau diminuarea efectelor generale ale acțiunilor de inducere în eroare ale (in)amicilor sau prin exploatarea efectelor generate de acestea.

• Contrapropaganda - are ca scop demascarea încercărilor (in)amicilor de a desfășura acțiuni de propagandă și a scopurilor acestora.

• Acțiunile de contrainformații - contribuie la desfășurarea cu succes a operațiilor informaționale defensive prin furnizarea de informații și prin desfășurarea de activități care să protejeze informațiile proprii împotriva spionajului, sabotajului sau acțiunilor teroriste.

• Războiul electronic - protecția prin mijloace electronice presupune acele acțiuni care vizează minimalizarea efectelor folosirii mijloacelor electromagnetice. Sprijinul prin mijloace electronice contribuie la realizarea cu succes a avertizării, prin descoperirea, identificarea și localizarea surselor de energie electromagnetică ce pot constitui amenințări.

• Relațiile publice - contribuie la siguranța informațională prin difuzarea de informații, care descriu fapte și situații, în scopul contracarării acțiunilor de inducere în eroare și de propagandă ale (in)amicilor.

• Securitatea fizică - urmărește asigurarea unui grad de protecție fizică a infrastructurii informaționale și a unor capacități de reacție în cazul detectării atacurilor.

În concluzie, operațiile informaționale defensive se concentrează pe protecția propriei informații, a proceselor bazate pe informație, a sistemelor de comandă-control și a celor de comunicații și informatică. Această protecție trebuie să fie adaptată pentru orice tip de (in)amic, în orice situație (pace, criză, conflict) și vizează patru componente: protecția infrastructurii informaționale, descoperirea atacurilor, restaurarea funcțiilor vitale și reacția la atacuri. Integrarea tuturor componentelor enumerate este esențială.

Operațiile informaționale ofensive implică folosirea integrată a capacităților și activităților desemnate, sprijinite de activitatea informativă *(itelligence)*, cu scopul de a afecta factorii de decizie (in)amici și de a promova obiective specifice.

Capacitățile folosite în acest scop includ (dar nu se limitează numai la ele) următoarele elemente:

• Operațiile psihologice - sunt destinate transmiterii anumitor informații și indicații către exterior, în scopul influențării atitudinilor, motivațiilor, raționamentelor și, în final, a comportamentului altor entități. Pot lua forma unor poziții exprimate la nivel politic sau diplomatic, unor comunicate, anunțuri, difuzării de broșuri, manifeste, emisiuni de radio și T.V. etc.

• Inducerea în eroare - vizează factorii de decizie prin afectarea proceselor și sistemelor de culegere, analiză și difuzare a informațiilor de către (in)amici. Acest lucru presupune cunoașterea detaliată a (in)amicilor și a proceselor decizionale ale acestora. Elementul cheie îl constituie anticiparea. Acțiunile de inducere în eroare depind de modul de desfășurare a acțiunilor de asigurare informativă, în scopul identificării celor mai potrivite ținte pentru elaborarea unui scenariu credibil și pentru aprecierea eficacității planului de inducere în eroare.

• Războiul electronic - presupune acțiuni destinate distrugerii, neutralizării sau degradării capacităților electronice ale (in)amicilor sau reducerea capacității acestora de a utiliza în mod eficient spectrul electromagnetic. Protecția și sprijinul prin mijloace electronice reprezintă exemple de capacități care contribuie la promovarea și îndeplinirea unor obiective specifice.

• Relațiile publice - pot contribui la desfășurarea operațiilor informaționale ofensive prin difuzarea de informații corecte și oportune către auditoriul intern (propria organizație) și extern (publicul larg), prin informarea despre scopurile, posibilitățile și intențiile dorite. Documente oficiale precizează că *„activitățile de relații publice nu sunt folosite ca modalități de inducere în eroare sau ca modalități de dezinformare a auditorului intern sau extern"*[72].

Atacul fizic/distrugerea - se referă la folosirea mijloacelor de distrugere asupra țintelor informaționale, ca element component al efortului integrat reprezentat de operațiile informaționale.

Relațiile civili-militari - cuprind, în viziunea N.A.T.O., *„totalitatea activităților prin care factorii de decizie stabilesc și dezvoltă relații între forțele proprii și autoritățile civile, resursele și instituțiile din zonele amice, neutre sau inamice în care sunt desfășurate aceste forțe"*[73].

Scopul de bază al operațiilor informaționale ofensive este de a influența cunoștințele și credințele factorilor de decizie, pentru

[72] MC 402 N.A.T.O., Psyhological Operations Policiy", 07.04.1997
[73] MC 411 N.A.T.O., Civil-Milytary Operations Policiy", 1998

a le reduce voința și abilitatea de a decide și pentru a perturba procesul decizional.

MANAGEMENTUL PERCEPȚIILOR ȘI FACTORUL UMAN

Adevărul nu este doar ceea ce crezi că este, ci el rezidă în circumstanțele în care este spus, cui, de ce și cum este spus.

Vaclav Havel

Un aspect distinct al operațiilor informaționale ofensive îl constituie managementul percepției, proces care cuprinde discipline precum relațiile publice, diplomația publică, operațiile psihologice (PSYOPS), inducerea în eroare și acțiunile sub acoperire.

Managementul percepției țintește dimensiunea umană în politică și în situații de conflict, într-un mod în care armele fizice nu o pot face. Acesta este înțeles ca proces care determină acele acțiuni ce transmit și/sau împiedică accesul adversarilor la informație, pentru a influența emoțiile, motivele sau obiectivele lor, vizându-se, în final, materializarea acestora în comportamente și acțiuni favorabile inițiatorilor.

Diplomația publică este menită să convingă diferite audiențe asupra adevărului și raționalității politicii, intențiilor și acțiunilor unei alte entități. In general, diplomația publică funcționează pe căi tradiționale - dialog diplomatic și politic direct, conferințe de presă, comunicate de presă, interviuri ete. - dar viteza la care se desfășoară astăzi unele evenimente cere capacități de comunicare pe măsură. Liderii unor puteri mici sau actorii non-statali au în prezent la dispoziție posibilități de informare la fel de sofisticate ca și cele deținute de liderii marilor puteri. Poate cea mai semnificativă diferență față de trecut este faptul că oamenii au nevoie să fie conectați la tot ce se întâmplă pe întreg mapamondul.

Aceasta înseamnă o multiplicare a surselor și un acces cât mai rapid posibil.

O diplomație eficientă, care contribuie prin mijloacele sale specifice la „modelarea spațiul informațional", necesită luarea simultană în considerare a diverselor surse de informare, mesajelor transmise și audienței vizate.

Inducerea în eroare acționează diferit față de celelalte elemente ale managementului percepției. Dacă relațiile publice, diplomația publică și majoritatea formelor de operații psihologice caută să informeze și să convingă într-o manieră corectă, inducerea în eroare dimpotrivă, distorsionează deliberat sensul realității pentru adversarul declarat.

Legăturile implicite existente între PSYOPS și inducerea în eroare creează adesea confuzii din cauza lipsei familiarității cu cele două discipline. PSYOPS sunt caracterizate ca fiind „albe" „gri" sau „negre", în limbajul de specialitate, însă acest aspect nu se referă la conținutul de adevăr al mesajelor, ci mai de grabă la identitatea sursei: adevărată, neidentificată sau falsă. Dar, indiferent de sursă, scopul PSYOPS este de a furniza țintei acea informație reală și credibilă care să determine comportamentul dorit. Inducerea în eroare poate îmbunătăți furnizarea mesajelor către țintă prin folosirea unor informații reale și verificabile, ceea ce va spori credibilitatea mesajului, dar metodele folosite și informațiile transmise sunt de altă factură decât cele utilizate în PSYOPS.

Cu toate acestea, linia de demarcație dintre PSYOPS și inducerea în eroare este deseori greu de perceput, cele două discipline sprijinindu-se reciproc în practică.

Înțelegerea culturală a audienței-țintă este un element critic în realizarea credibilității. Un mesaj devine cu atât mai credibil cu cât este mai corect cultural, indiferent dacă este adevărat sau fals. Tehnologia disponibilă astăzi permite personalizarea mesajelor în funcție de țintă și de modul agreat de ea în receptare. Nu mai contează dacă mesajul este adevărat sau fals, dacă el este

ambalat și transmis corespunzător. Folosirea canalelor directe pentru distribuirea mesajelor poate, de asemenea, să sporească credibilitatea acestora. Pe acest fapt se bazează succesul inducerii în eroare, care preferă această cale de distribuire a mesajelor, în cazul PSYOPS este indicat ca unele mesaje să fie transmise și pe alte canale, dar nu în mod obligatoriu. Acest fapt se dovedește util, deoarece credibilitatea mesajelor depinde și de capacitatea adversarului de a verifica conținutul lor și pe alte căi decât cele anticipate. Realizarea unui nivel similar de credibilitate pentru mesajele destinate inducerii în eroare este mult mai dificil de realizat tocmai pentru că mediul informațional de azi permite țintei verificări multiple ale acestora.

Rezultatele experienței câștigate în urma conflictelor din ultimul deceniu, din perspectiva PSYOPS, au determinat recunoașterea acestora ca fiind o componentă importantă a planificării operațiilor militare. In ultimul timp, PSYOPS sunt recunoscute de planificatorii militari ca fiind un ingredient absolut necesar în ceea ce se numește *„invitational operations"*, unde cerința de bază a îndeplinirii misiunii o reprezintă consensul popular (de exemplu, operațiile umanitare sau de menținere a păcii).

Diferitele elemente constitutive ale managementului percepțiilor nu pot fi implementate corespunzător în practică în afara capacităților de a înțelege (și în final de a ținti) modul de asimilare și procesare a informațiilor de către oponenți. Prin monitorizare continuă, dinamică și prin țintirea focalizată a sistemelor de informații (computerizate sau nu) ale (in)amicului se obțin cunoștințe detaliate despre infrastructura fizică și interrelațională ce înconjoară ținta. Analiza factorului uman necesită construcția unui tablou general al mediului informațional care înconjoară ținta, precum și un tablou general al infrastructurii umane, a statului-țintă sau a unei anumite organizații (grup) țintă.

Prin analiza factorului uman se înțelege un cumul de elemente psihologice, culturale, comportamentale precum și alte atribute

umane care influențează luarea unei decizii sau a informațiilor pe care le deține o persoană și interpretarea individuală sau de grup a acestora. Analiza factorului uman are un rol cheie în desfășurarea operațiilor de-management al percepțiilor.

Ea se axează în principal pe trei tipuri de elemente existente sau potențiale ale sistemelor adversarului:

- autoritatea factorilor de decizie
- structurile naționale sau de grup implicate în luarea deciziei
- procesul decizional în sine

Analiza acestor elemente presupune elaborarea unui studiu detaliat al naturii și caracteristicilor regimurilor analizate sau a grupului țintă. Prin aceste analize trebuie înțelese locul, intensitatea și expunerea factorilor externi, de mediu, factori care pot influența procesul decizional și acțiunile liderilor sau grupurilor.

Urmărirea, analiza și evaluarea aspectelor pur psihologice reprezintă cheia analizei factorului uman. In acest tip de analiză se ține cont și de faptul că anumite elemente culturale ale sistemelor decizionale analizate implică și înțelegerea complexului istoric și a influențelor manifestate de-a lungul secolelor.

Astfel, un anumit tip de regim va genera un tip specific de comportament în luarea deciziilor. Acest fapt implică obligatoriu analizarea atât a caracteristicilor sociale care includ aspecte demografice, lingvistice, componență etnică, influențe naționale și sub-naționale, cât și impactul pe care îl are geografia asupra naturii și culturii unui popor.

Studiul conducerii presupune înțelegerea detaliată a unei arii foarte largi de probleme cum ar fi:

- înțelegerea personalității intrinseci și a temperamentului liderilor politici, militari etc;
- analiza și interpretarea obiectivelor generale și specifice și aspirațiile urmărite în mod individual sau a celor de grup;
- înțelegerea credințelor, sistemelor de valori și a tendințelor țintelor vizate Intre o organizație de tip birocratic, structurată ierarhic și un grup terorist, de exemplu, nu numai diferențele

culturale sunt importante, ci și structurile relaționale din interiorul acestora. Acestea vor face în mod special obiectul analizei factorului uman.

Prin acest tip de analiză pot fi anticipate acțiunile individuale ale decidenților (ceea ce oferă posibilitatea ameliorării sau îmbunătățirii propriilor O.I), dezvoltarea lor profesională, stilul decizional al conducerii, pe scurt, un întreg profil psihologic și o întreagă evaluare a (in)amicului.

ELEMENTE ALE UNEI STRATEGII DE INFLUENȚARE

Schimbarea este o lege a firii. Cei care privesc doar spre trecut sau doar spre prezent vor rata, cu siguranță, viitorul.

John F. Kennedy

Exportată intens de S.U.A., dar greu de digerat pentru multe din statele europene membre N.A.T.O., revoluția în afacerile militare (R.A.M.) implică pentru o țară ca România, o schimbare de paradigmă în gândirea și practica strategică, dificilă în contextul actual, în care politicile structuraliste de reformă și modernizare a sistemului de siguranță națională sunt, în esență, de natură energetică.

Necesitatea unui proces de tip R.A.M., în cadrul sistemului de siguranță națională al României în anii următori, trebuie motivată de o viziune strategică de ansamblu, comună cu cea euro-atlantică.

Dar cum poate fi creată o astfel de perspectivă când Statele Unite și Europa au viziuni destul de diferite?

Care va fi modelul strategic de urmat?

Asimetria dintre strategia militară, capacitățile și tehnologia S.U.A., pe de o parte, și partenerii săi militari, aliații N.A.T.O., de cealaltă parte, constituie un motiv de preocupare pentru tot mai mulți analiști politico-militari și lideri politici. Înțelegerea

acestei diferențe este importantă pentru România în procesul de integrare euro-atlantică.

Temeiuri și polemică

Din perspectiva asimetriilor și tendințelor de bipolarizare ale sistemului euro-atlantic de securitate este dificil, cel puțin în etapa actuală, a se decide asupra modelului strategic de aplicat în continuarea reformei (cu toate că, în practică, abundența de date și oferta de know-how fac mai atractiv și ușor de adoptat modelul american).

Un start adaptat și adecvat în R.A.M. înseamnă promovarea unui comportament politico-militar proactiv **(strategia acțiunii),** utilizând instrumente de analiză, instruire și sprijin decizional **(strategia optimalității)** și desfășurând acțiuni de protejare și influențare a informațiilor, proceselor și sistemelor informaționale proprii, ale (in)amicilor **(strategia de influențare),** prin operații informaționale.[74]

Având un rol de descurajare, în absența altor elemente credibile, **strategia acțiunii** trebuie să permită creșterea, după împrejurări, a puterii sau a influenței țării în exterior. Aceasta presupune o reînnoire simultană a strategiei directe, în care forța armată joacă rolul cel mai important și a strategiei indirecte în care, fără a fi exclusă, forța armată se află într-un plan secundar.

Strategia acțiunii este stimulată de apariția unor operații noi la nivel strategic, al căror scop nu este în esență hotărât pe calea armelor sau a confruntării fizice și care se înscriu în mai multe strategii indirecte. Acest aspect antrenează în fapt o diversitate de „câmpuri de operație"[75] în care trebuie să se desfășoare angajamentele.

---

[74] Diferența nu rezidă neapărat într-un accent pus diferit pe tehnologia informațională, ci este mai mult o chestiune de paradigmă.

[75] Conform unei tipologii prezentate de Felix Faucon, câmpurile operaționale se împart în câmpuri conceptuale, psiho-sociologice, geopolitice, geografice, fizice câmpuri ale sistemelor de decizie și de informație („Guerre de lp—infonnation ou operations d'infonnation?", *Defense Nationale,* nr. 3, 1998).

În noul context, determinarea capacităților strategice necesare și planificarea siguranței naționale trebuie să înceapă printr-o analiză a câmpurilor de operație în care acestea pot acționa cu eficacitate.

Analiza invită la redimensionarea conceptului clasic de „operație" dincolo de limitele geografice impuse de conținutul său tradițional: „zonă de operații", punând în discuție inclusiv limitele temporale.

Strategia optimalității. In contextul actual de redimensionare și optimizare a structurilor de siguranță, lansarea procesului de dezvoltare consistentă și pragmatică a domeniului modelare-simulare apare ca o necesitate fezabilă.

Prin componentele sale fundamentale (modelele, simularea în teren, jocurile de război și politici militare, simularea virtuală), acest domeniu poate fi unul dintre pilonii procesului de modernizare și reformă și, totodată, poate asigura o optimizare a proceselor și activităților specifice structurilor care au atribuții în domeniul siguranței naționale a României.

De asemenea, prin utilizarea efectivă a instrumentelor de analiză și sprijin decizional, maniera de rezolvare a problemelor de orice natură și palier ierarhic poate fi îmbunătățită, dând posibilitatea factorilor de decizie să evite concentrarea asupra rezolvării crizelor imediate și să se îndrepte spre o stare de anticipare a evenimentelor.

Strategia optimalității trebuie corelată cu o politică dinamică de dezvoltare a infrastructurii informaționale naționale, al cărei accent să cadă pe protejarea infrastructurii critice și pe deplasarea priorităților spre zona informatică a serviciilor de informare-documentare, sinteză și fuziune a cunoștințelor.

Strategia de influențare. Evenimentele ultimului deceniu pot sugera desfășurarea unor subtile operații informaționale în spațiul geostrategic de interes al României.

Principalele caracteristici ale reacțiilor la aceste acțiuni au fost, din diverse cauze, unilateralitatea ripostei, lipsa de coordonare

și absența unei viziuni globale, integratoare. Unul din cele mai mari pericole este acela că, uneori, probabil nici nu s-a conștientizat faptul că factorii de decizie au fost ținta unor astfel de acțiuni. Există, de asemenea, un risc al „interoperabilității" care se poate formula astfel: cine are o cunoaștere foarte bună despre arhitectura sistemelor de comunicații și informatică, substanța deciziei și transformările logice dintr-un sistem de conducere ar putea determina transformările dorite.

Totodată, în ultimii ani, în „spiritul interoperabilității", au fost importate diverse concepte și modele militare occidentale, într-un mod destul de artificial, fără o înțelegere și adecvare de profunzime și, în consecință, cu un succes discutabil.

Ansamblul orientărilor și deciziilor în materie de reformă a organismului militar, necesită, dincolo de procesul cunoscut sub numele „Military Action Plan", de standardele deja clasice de interoperabilitate, de strategia de imagine etc., o aliniere și adecvare la „schimbările de fond ale naturii conflictelor".

Strategia de influențare presupune dezvoltarea adecvată a domeniului „operații informaționale" pentru a se ajunge, la nivel național, la stadiul în care să se dispună de un cadru legislativ și metodologic, precum și de un ansamblu de structuri și mijloace specializate, capabile să descurajeze pe căi și prin mijloace informaționale acțiunile contrare intereselor naționale, să contracareze efectele acțiunilor informaționale la nivelul factorilor de decizie și al sistemelor informaționale.

In concluzie, interesul pentru „noua cultură a conflictelor" și „revoluția informațională" - cu determinări majore privind extinderea responsabililătilor organismului militar în materie de siguranță națională, proiectarea unor capacități strategice și redefinirea proceselor de comandă și control din perspectiva asimetriei - reclamă o luare în considerare a următoarelor aprecieri, care. integrale, construiesc un posibil cadru teoretic general de reflecție:

• „Utilizarea forței în mod eficient, pe o scară mai mare sau mai mică, se face mai mult pentru a preveni escaladarea

conflictelor decât pentru o confruntare directă de forțe militare."[76]

• „Orice conflict poate fi tolerat dacă nu produce victime omenești" – aserțiune susținută de teoria campaniilor informaționale.

• Trecerea de la un concept clasic de organizare la unul postmodern presupune „schimbarea caracterului forțelor armate, care nu trebuie să mai reprezinte expresia - națiune în armată - ci să fie mai degrabă un corp de profesioniști."[77]

• Tehnologiile informaționale, ca o condiție pentru acțiunea militară eficientă, sunt dimensiuni esențiale în planul evoluției gândirii și practicii militare. Pe măsură ce aceste tehnologii se schimbă, se schimbă și contextul în care sunt făcute alegerile de politică, strategie și doctrină militară. Pe măsură ce sunt elaborate noi tehnologii, se modifică și sfera alternativelor posibile privind planificarea apărării și acțiunea militară propriu-zisă.

Revoluția informațională oferă tehnologii care modifică continuu influența binomului timp-spațiu și contribuie substanțial la creșterea complexității; transformă liniarul în neliniar și secvențialul în simultan. Teoria complexității și nelimaritatea (viziunea neo-clausewitziană) - generatoarea unei noi paradigme în gândirea militară - impun o reconstrucție a mediului militar.

Noua cultură a conflictelor contribuie la consolidarea curentului centrat pe filosofia lui Sun Tzu: gândire simplă, bazată pe inducere în eroare și cunoașterea minții (in)amicului. Principiile lui Sun Tzu, puse în acord cu elementele tehnologice, pun bazele unei noi strategii de competiție/negociere și de rezolvare a crizelor.

Următoarele afirmații încearcă să contureze (sau mai mult să

[76] E. Luttwak, „The Crisis of Classic Military Power & the Possible Remedy of Post-Heroic Intelligence-Based Warfare", *The Information Revolution & International Securtîy*, Center for Strategic & International Studies, 1998

[77] R.Jervis, „Signaling / Perception in the Information Age", *The Information Revolution & National Security*, Strategic Studies Institute, 2000

sugereze) un cadru general de abordare a problematicii „operațiilor informaționale":

• Există, în prezent, posibilități de influențare a politicii diferitelor entități (state, actori transnaționali, organizații, indivizi etc.), fără a se folosi forța armată. Există forme de conflict în care războiul convențional este marginal, dacă nu chiar absent. Definiția clausewitziană a războiului se erodează treptat. „Operațiile informaționale" devin posibilități din ce în ce mai atractive de promovare și menținere a intereselor (naționale, organizaționale, individuale etc.).

• Conflictele sunt mai mult decât „ciocniri de tehnologie". Supremația tehnologică nu a putut împiedica nici înfrângerea Olandei în Indonezia, a Franței în Indo-China și Algeria, a Americii în Vietnam, a Uniunii Sovietice în Afganistan, a Rusiei în Cecenia și nici asigura succesul N.A.T.O. în Kosovo. Aceste episoade confirmă faptul că superioritatea tehnologică nu este o garanție implicită a victoriei pe câmpul de luptă, și cu atât mai puțin la masa negocierilor. Tehnologia este importantă, dar nu decisivă.

Vrând-nevrând, globalizarea și „societatea informațională" devin realități presante, generatoare de forme noi de agresiune (informațională), cu implicații în redefinirea conceptului de securitate națională (prin adăugarea unei dimensiuni noi - „securitatea informațională"[78]).

Dacă „societatea informațională" - spre care ne îndreptăm - este un factor major de generare a prosperității și o cerință vitală pentru integrarea europeană, atunci „securitatea informațională" reprezintă un factor-cheie pentru protejarea intereselor naționale.

Acesta este un alt motiv pentru care trebuie să vorbim de război și operații informaționale.

[78] Prin securitate informațională se înțelege „starea de protecție a necesităților de natură informațională ale individului, societății și statului, care să permită asigurarea satisfacerii acestora și evoluția lor progresivă, independent de prezența amenințărilor de natură informațională, interne și externe", http/www.ndu.edu/inss/siws/cont.html

Este evident, de asemenea, că spectrul actual al crizelor și conflictelor include, pe lângă spațiul fizic, obișnuit nouă, și spațiul virtual.[79] Trebuie să ne pregătim să facem față amândurora, pentru că spațiul virtual este o cale importantă pentru o entitate mai mică de a-și crea o contrapondere în fața unor entități mai mari sau/și mai avansate din punct de vedere tehnologic. Totodată, spațiul virtual este o soluție complementară viabilă de management al riscurilor la adresa siguranței naționale.

Nu în ultimul rând, a vorbi despre necesitatea utilizării operațiilor informaționale - ca factor de descurajare la nivel strategic și catalizator către un comportament politico-militar proactiv - presupune conștientizarea faptului că primul pas în direcția unei deschideri trebuie să îl reprezinte spargerea rezistenței la schimbare.

Inserarea de noi paradigme (O.I. de exemplu) în procesul complicat și sinuos al modernizării este importantă, deoarece acestea sunt acțiuni și instrumente absolut necesare în stabilirea condițiilor, planificarea și conducerea eforturilor în domeniul siguranței naționale.

O.I. sunt un instrument care asigură un avantaj cert în mediul geostrategic actual - un mediu tot mai dependent de informație și de infrastructură care asigură tipul și volumul informațiilor de care este nevoie. Sistemele naționale de bază (politic, social, economic, militar și ecologic) depind de informație și de instrumentele informaționale (comunicații, automatizare). Această dependență constituie, în egală măsură, putere și vulnerabilitate. Pe de o parte, dependența înseamnă a avea posibilitatea racordării siguranței naționale la realitățile occidentale ale „revoluției în afacerile militare"[80], având la dispoziție tehnologie de vârf. Dar,

[79] Obișnuința cu (in)amici și/sau competitori bine conturați generează pericolul ignorării acelora care se manifestă în spațiul virtual.

[80] „Revoluția în afacerile militare" implică folosirea tehnologiei informaționale pentru a obține *superioritatea informațională*, prin cunoașterea unui spațiu de conflict, în toate dimensiunile sale, și prin asigurarea celei mai bune reacții, la orice nivel.

pe de altă parte, aceasta înseamnă vulnerabilitate la atacurile care ar putea provoca efecte dezastruoase la nivelul propriului proces decizional.

O.I., ca modalități de acțiune pe timp de pace și în situații de criză și conflict, reprezintă un punct de plecare radical diferit față de prezent și constituie, într-adevăr, o revoluție a modului de luptă.

Trebuie luat în calcul și faptul că există o importantă teorie occidentală în acest domeniu și chiar o politică N.A.T.O.[81] privind O.I.. Orice viitoare teorie proprie O.I, chiar dacă va adopta sau adapta litera occidentală, prin spiritul său trebuie să ne ajute să percepem corect amploarea transformărilor induse de „revoluția informațională", să înțelegem că trebuie să ne dezvoltăm capacități intelectuale și tehnice adecvate pentru a duce O.I și să conștientizăm că (in)amicii și/sau partenerii noștri vor vedea, cu siguranță, vulnerabilitățile noastre informaționale și vor încerca să le exploateze.

O dezvoltare generală proprie O.I. trebuie să ia în calcul și să particularizeze cel puțin două teorii - teoria agregării și teoria neliniarității - concepte esențiale în înțelegerea acțiunilor informaționale. Teoria agregării include interacțiunea lucrurilor (indivizi, organizații etc.) și a legăturilor (elemente fizice, activități etc.). Când se combină lucruri și legături rezultă efecte importante, mult mai importante decât dacă ar fi rămas separate.

Agregarea trebuie studiată din perspectiva integrării unor domenii, discipline și tipuri de acțiuni distincte în cadrul unei O.I. - acțiunile psihologice, (contra)informațiile, (contra)inducerea în eroare, relațiile publice, relațiile militari-civili, (contra)acțiunea electronică, securitatea și siguranța informațională, securitatea operațiilor, securitatea fizică, (contra)propaganda și acțiunile speciale. Înțelegerea teoriei agregării, modelarea și simularea proceselor militare din perspectiva neliniarității (teoria haosului și teoria complexității), precum și înțelegerea modului de a crea

[81] Documentul MC-422 *„Information Operation Policy"*, adoptat la 22.01.1999

intenționat efecte de nivel doi și trei, toate acestea deschid ușa planificării și executării unor O.I. care să descurajeze și să reducă riscurile polilico-militare.

In ciuda gravității problemei, suntem, momentan, la începuturile examinărilor teoretice [82], necesare dezvoltării unei teorii și practici viabile a operațiilor informaționale, care să fixeze un cadru instituționalizal de abordare și adoptare a unei reacții politico-militare în situații de criză și conflict specifice epocii informaționale (dacă acceptăm că mediul geostrategic actual se îmbogățește cu „trăsături informaționale").

CONCLUZII

Rapida evoluție a tehnologiei informației a dus la o schimbare de paradigmă privind natura conflictelor. Războiul informațional este acum o noțiune practică pentru multe națiuni. Costul necesar pentru obținerea de capacități credibile defensive privind R.I. este relativ scăzut, cu siguranță mult mai mic decât cel necesar pentru realizarea unei siguranțe naționale convenționale. Iată de ce capacitățile în domeniul R.I. sunt o alegere atractivă pentru un spectru larg de entități tradiționale sau moderne.

R.I. are la bază o strategie integratoare care recunoaște importanța și utilitatea informațiilor în comanda și controlul sistemului de siguranță națională și în implementarea strategiei de securitate națională. R.I. exploatează oportunitățile și vulnerabilitățile inerente dependenței crescânde de informație, concentrându-se asupra sistemelor și tehnologiei informaționale.

R.I. nu este un fenomen cu care se confruntă doar țările evoluate. Structura actuală a sistemului internațional se îndreaptă spre o relație de interdependență statală tot mai accentuată, în

[82] In competiția pe plan conceptual și doctrinar, în raport cu temele de reflecție majore actuale (teoria neo-clausewitziană a neliniarității războiului, modelarea și simularea acțiunilor militare, operațiile informaționale, managementul riscurilor etc.) gândirea militară românească manifestă o inexplicabilă rămânere în urmă.

care sunt angrenate atât statele dezvoltale, cât și cele mai puțin dezvoltate.

Modul de a înțelege și de a percepe fenomenul R.I. diferă de la o țară la alta în funcție de realitățile proprii fiecăreia și de interesele pe care consideră că le poate promova cu ajutorul acestui instrument.

Trecerea în revistă a câtorva puncte de vedere aparținând unor state care au preocupări în domeniu!!! lasă să se degajeze cel puțin patru idei comune.

In primul rând, R.I. poate fi înțeles doar în cadrul întregului complex de schimbări. El nu influențează doar sectorul militar, ci întreaga societate și comunitate internațională.

Unul dintre efectele tehnologiei informaționale este crearea spațiului virtual, ca o nouă dimensiune în care poate fi dus războiul. Spațiul virtual are elemente de bază inseparabile: forțele armate, națiunea și comunitatea internațională. Toate nivelurile de comandă și control pot fi atacate și, în consecință, trebuie să fie apărate. La toate nivelurile, omul este cel care are puterea de decizie finală. Acest aspect face din conceptul de „influență" o opțiune și un pericol. Statele moderne se confruntă cu o dilemă. Pe de-o parte, digitalizarea este un stadiu evolutiv firesc spre care tind societățile moderne și, pe de altă parte, aceste progrese creează noi și serioase vulnerabilități.

In al doilea rând, R.L este o adevărată problemă. El pune sub semnul întrebării o serie întreagă de „vechi adevăruri". Nu există soluții ușoare. Un prim pas ar fi înțelegerea faptului că există riscuri. Un alt pas constă într-o evaluare atentă a vulnerabilităților. Tehnologia aduce multe foloase, dar și o mulțime de greutăți.

In al treilea rând, planificarea și ducerea unui R.I. strategic este, în orice caz, un proces complex în care, așa cum este cazul cu toate formele de război, informațiile și serviciile de informații sunt un factor-cheie pentru dezvoltarea și desfășurarea unor planuri și operațiuni efective de R.L, fie pentru dezvoltarea unor măsuri proprii de protecție a sistemelor militare, fie pentru realizarea unui sistem de degradare a capacităților acționale ale unui (in)amic.

Nu în ultimul rând, studiile de vulnerabilitate, analizele efectuate pentru caracterizarea amenințării, simpozioanele internaționale dovedesc importanța acordată de comunitățile de informații acestui nou fenomen. Deja amenințarea informațională nu mai este doar problema specialiștilor din domeniul militar. Mass-media începe să propage efecte devastatoare ale acestei arme noi, prea puțin convenționale.

R.I. a acordat, de altfel, un plus de autoritate actorilor și aspectelor netradiționale. Organizațiile mici cu buget restrâns, sunt acum capabile de o mai mare agresivitate și influență decât ar fi putut prezice teoriile relațiilor internaționale.

Din acest motiv, conceptul tradițional de siguranță națională trebuie să evolueze spre ceva mai flexibil, mai proactiv și mai dinamic. Pregătirea trebuie să vizeze cel puțin trei niveluri:

- politic - să se aibă imaginea de ansamblu a amenințărilor la adresa infrastructurii informaționale la nivel național și internațional;
- de *intelligence* - să se înțeleagă indicatorii și avertizările și să se poată conlucra cu planificatorii strategici;
- de sistem - să se recunoască atacurile și să se știe cum să se reacționeze;

În final, se poate afirma că:

- Noua cultură a conflictelor se cristalizează odată cu crearea noii dimensiuni cibernetice și cu apariția noilor concepte și instrumente strategice, printre care operațiile informaționale strategice, derulate prin intermediul operațiilor psihologice complexe, conflictelor mediatice, atacurilor digitale sau managementului percepțiilor.
- Strategiile asimetrice centrate pe acțiuni informaționale defensiv-ofensive nu vor conduce la o forță de reacție mult mai puternică în sensul cantitativ clasic, ci mai degrabă la o mai mare abilitate de folosire a forței neconvenționale pe timp de pace și în situații de criză, pentru menținerea și promovarea intereselor naționale și chiar la posibilitatea de planificare a mijloacelor clasice

într-o mai mare măsură, cu discernământ și acuratețe. Dacă aceste considerații se corelează cu realitatea efortului guvernamental de dezvoltare a societății informaționale, atunci provocările pentru decidenții și planificatorii din sistemul siguranței naționale de abia acum încep.

• Totalitatea operațiilor informaționale desfășurate în timp de criză sau conflict în scopul atingerii unor obiective sau influențării unor anumite ținte poartă numele de „război informațional".

• Războiul de comandă-control este aplicarea în plan militar a operațiilor informaționale.

• Operațiile informaționale pot fi înțelese doar în cadrul întregului complex de schimbări. Ele nu influențează doar sectorul militar, ci și întreaga societate și comunitate internațională.

• Operațiile informaționale nu se confundă cu operațiile de informații, care sunt desfășurate exclusiv de structurile de informații.

• Operațiile informaționale pot contribui la integrarea elementelor militare ale puterii naționale cu celelalte elemente, în scopul atingerii obiectivelor naționale.

• Unul dintre cele mai mari câștiguri, ce poate fi exploatat de pe urma folosirii operațiilor informaționale, este abilitatea lor de a preveni dezvoltarea unei crize în conflict. In acest sens, operațiile informaționale trebuie să fie desfășurate încă de pe timp de pace și necesită atât sprijin politic, cât și militar.

Totodată, operațiile informaționale pot fi folosite pentru întreruperea sau chiar ruperea legăturilor de tip social, țintele fiind transportul, comunicațiile, energia, instituțiile financiare etc. prin *„folosirea ciberspațiului* [83]*, pentru afectarea operațiilor militare strategice și pentru aducerea de prejudicii infrastructurilor informaționale naționale"*. Un astfel de atac asupra societății poate

[83] John Arquilla și David Ronfeldt, *In Athena's Camp, Preparing for Conflict in the Information Age, http://www.rand.org./publications/MR/MR880/contents.html*

avea consecințe foarte grave. În acest context, nu este deloc surprinzător faptul că multe țări studiază aceste riscuri potențiale.

În ceea ce privește efectele utilizării operațiilor informaționale, prima observație este costul relativ scăzut al unui atac asupra sistemelor informaționale și comunicațiilor în rețea. Acesta este trivial în comparație cu mijloacele militare convenționale. O combinație de computere și minți pregătite și pline de imaginație este suficientă pentru a produce efecte operaționale majore (evident, la nivelul entităților care depind major de infrastructură).

Conștient sau nu, la toate nivelurile, se acționează în prezent pentru întărirea interoperabilității și reducerea măsurilor de protecție în beneficiul vitezei. Toate aceste mecanisme, într-un fel sau altul, favorizează creșterea vulnerabilităților și a intruziunilor, în contextul în care factorul timp în planul contramăsurilor, tinde spre zero (dacă un atac convențional cere timp pentru organizarea, pregătirea și dispunerea forțelor, un atac informațional poate să înceapă la puțin timp după decizia de a se desfășura).

Operațiile informaționale sunt un mod de gândire și... o invitație la reflecție. Este momentul unei schimbări de paradigmă!

SIGURANȚA INFORMAȚIONALĂ EXPERIENȚA CANADIANĂ

TITT T. ROMET*

Această lucrare va descrie inițial elementele unui larg cadru conceptual care a fost utilizat. El va descrie apoi conceptul specific dezvoltat în cadrul CF (Forțelor Canadiene) și o evidențiere a structurilor ce au fost formate. Lucrarea trece în revistă lecțiile învățate, cele ce sunt în curs de învățare și cele ce urmează să fie învățate precum și dificultățile avute în abordarea holistică privind dezvoltarea unui program de operații informaționale, atât la nivel militar cât și la nivel guvernamental.

Cu cinci ani în urma, Forțele Canadiene (CF) s-au confruntat cu decizia de a integra operațiile bazate pe informații în activitatea militară curentă. Cu evoluția rapidă a tehnologiilor de comunicație și tehnologiilor calculator, informația a fost recunoscută ca o resursă strategică ce trebuie administrată efectiv.

Canada era deja integrată sub aspectul rețelelor cu SUA în numeroase domenii înrudite cum ar fi telecomunicațiile și sistemul bancar. Confruntată cu creșterea globală a schimburilor comerciale și de informație prin intermediul extinderii rețelelor de comunicații, a fost necesar să se înțeleagă faptul că imaginea tradițională a granițelor nu mai există.

Așteptările nu au fost create numai în sectorul militar ci și în cel guvernamental și privat unde informația poate fi obținută instantaneu, analizată și schimbată. Internetul a devenit rețeaua prin care informațiile personale (private), informațiile de afaceri

* Consultant privat și cercetător, anterior cercetător științific al apărării, Canada

și chiar informații militare (senzitive) ar putea fi schimbate. Atât eficiența noastră economică cât și militară a fost sporită pe baza sistemelor informaționale automate și a rețelelor.

Mai mult, pentru reducerea costurilor și crearea de noi elemente de eficiență, militarii au integrat tot mai mult tehnologii militare în sistemele lor militare. Noi descriem aceste fenomene ca fiind „transformarea civilă a militarilor".

Cu militarii SUA mișcându-se foarte rapid în acest nou domeniu, pe care ei l-au numit inițial „Război informațional", Canada a avut nevoie să abordeze principalele probleme cu care se confruntă. CF a înțeles că nu are resursele umane și financiare pentru a urma abordarea SUA și că are nevoie să dezvolte un cadru conceptual în conținutul căruia principalele cerințe să poată fi analizate și implementate.

Este general acceptat că apariția activității bazate pe informații este legată direct de progresele tehnologice care au avut loc pe parcursul ultimelor decade și ale aplicațiilor lor. Domeniile tehnologice cheie, care se află în spate, sunt comunicațiile, senzorii și calculatoarele.

Extinderea și varietatea comunicațiilor care au fost vast dezvoltate îmbunătățesc opțiunile, complexitatea și caracterul critic al informațiilor pe care le vehiculează. Prin mijloacele de transmisie care oferă alegeri mai multe, ce variază de la fără fir, cabluri de cupru în bandă largă, la fibre optice, disponibilitatea progresiv crescătoare a numărului de canale, a lărgimilor de bandă și a tipurilor de circuite (ex. prin satelit, cablu TV) s-a extins domeniul și s-a scurtat timpul în care informația poate fi schimbată.

Informația este acum disponibilă printr-un mare număr de surse, și în special din perspectiva militară, de la senzori ne-umani. Întreg spectrul electromagnetic poate fi exploatat pasiv sau activ prin mijloace de culegere diferite cum ar fi radio, radar, infraroșu / electrono-optic și radar cu aparatură sintetică. În paralel, contramăsurile au evoluat de asemenea la o mascare mai bună, inducerea în eroare sau ascunderea obiectelor de interes.

Evoluția constantă a componentei hardware și software a calculatorului prin creșterea dimensiunii, puterii și aplicabilității odată cu reducerea în dimensiune și cost, reprezintă o reamintire zilnică a dificultății de a sta în domeniul de vârf al tehnologiei informației.

Nu a evoluat numai baza tehnologică pentru societatea bazată pe informație ci și sistemele și organizațiile care utilizează tehnologie au crescut în număr și complexitate. Suportul de știri acoperă în prezent activitatea globală pentru 24 de ore, 7 zile pe săptămână fiind în creștere, și este disponibil în mod egal pentru un număr mai mare de populație din întreaga lume.

Rețeaua Internet a devenit substratul de conduită pentru o mare parte a schimbului de informații și comunicații. Ea a evoluat dramatic de la începuturile ei, o propunere a corporației RAND ca rețea de supraviețuire nucleară utilizând elemente individuale nesigure sau elemente vulnerabile așa încât capabilitatea și funcționalitatea sistemului să poată să se manifeste. Astăzi, cererea de informații prin intermediul Internet se suprapune cu preocupările pentru securitatea și integritatea informației, sau credibilitatea sursei. Consecvent, chiar astăzi, informația poate fi expusă interceptării, distorsionării sau furtului.

Comerțul electronic este domeniul economic care a crescut cel mai rapid. Legal sub formă de bani, stocuri, bunuri și multe alte tranzacții se realizează acum electronic sau sunt numai o intrare electronică într-o bancă de date. Comerțul Canadei, (și astfel cel al CF), este în mare măsură dependent de intimitatea și precizia Internetului și a echivalenților lui comerciali.

În timp ce SUA a început explorarea și activitatea ei pentru Operații Informaționale din domeniul militar, Canada a ales ca punct de start mediul informațional global (GIE). GIE a fost definit de indivizi, organizații sau sisteme în afara sferei de control militar, însă cuprinde mediul informațional militar (MIE) definit separat și distinct.

S-a considerat că toate „operațiile" au loc în GIE și din cauza

progreselor tehnologice, operațiile militare pot fi vizualizate, analizate și diseminate audienței globale în timp aproape real. De fapt poate fi arătat că informația ar putea fi distribuită mai repede prin intermediul legăturilor comerciale decât prin mijloace guvernamentale sau militare.

Pentru a sprijini GIE, există infrastructura de informație globală (GII) care este o interconectare a rețelelor de comunicații, calculatoare, baze de date și consumatori electronici ce permit accesul la informație a unei audiențe largi. Ea este legată global și este caracterizată de unirea rețelelor și tehnologiilor informaționale militare și civile.

Există în cadrul GII, infrastructura informațională națională (NII), care constă într-o serie de componente ce includ rețelele informaționale publice (guvernamentale) și private sprijinând preocupările, activitățile și organizațiile naționale. Nu există granițe discrete între GII și NII; de fapt, accesul global la informație devine tot mai critic pe măsura globalizării piețelor, resurselor și economiilor. Infrastructura informațională a apărării (DII) este inclusă în cadrul infrastructurilor menționate mai sus, oferind suport pentru misiuni, comandă și control și rețele de intelligence pentru militari.

În cadrul conceptual a fost stabilită o structură care ar putea să se adreseze preocupărilor de intimitate, confidențialitate și procesului de luare al deciziei. Deoarece au fost dezvoltate multe modele diferite și sisteme pentru a descrie luarea deciziei ele au aceleași elemente de bază comune:

a. achiziția datelor;

b. prelucrarea șirurilor de date în informații utile care vor conduce la înțelegere;

c. compararea cu starea existentă sau curentă;

d. decizia de implementare, direcționare etc.

Este important de înțeles că în cadrul ciclului de luare a deciziei există două entități distincte aflate în legătură care

contribuie în final la luarea deciziei. Există un *domeniu informațional* care este compus din trei elemente:

a. un set specificat de bunuri informaționale;

b. utilizări autorizate ale informației;

c. o politică de securitate ce guvernează utilizarea bunurilor informaționale.

Ca un exemplu, bunurile informaționale ar putea să includă toate înregistrările medicale și informația despre un individ în cadrul unui plan de sănătate elaborat la nivel guvernamental. Politica de securitate ar trebui să specifice cum este informația protejată, cine are acces, cum este informația stocată, prelucrată, etc.

Cealaltă entitate este *sistemul informațional* actual, care cuprinde componentele de prelucrare și comunicare ce trebuie să încorporeze elementele și politicile de securitate scoase în evidență în domeniul informațional.

Structura actuală a sistemului informațional poate fi separată în trei straturi care se suprapun unul peste altul și sunt bazate pe funcția lor: fizică, logică și semantică. Această împărțire pe categorii a fost folositoare în înțelegerea vulnerabilităților informației în cadrul oricărei structuri informaționale. La bază se află **stratul fizic** care poate fi descris de elementele hardware ale sistemului informațional.

Aceasta ar putea include clădiri, calculatoare, echipamente de comunicație și chiar personal. Această imagine conduce natural la conceptul de realizare a analizei „legături și noduri". Stratul din mijloc este **stratul logic** care constă în modul cum structura este operată, pachetele soft, sistemele, prelucrarea datelor în informații și în final în cunoștințe, distribuirea informațiilor și procedurilor de operare. Al treilea și cel mai înalt nivel se numește **nivelul semantic** și reprezintă conținutul și interpretarea informației incluse în cadrul sistemului informațional.

Nivelul fizic este vulnerabil la distrugerea fizică și este obiectul sistemelor de arme militare tradiționale. Deoarece infrastructurile militare și civile devin tot mai integrate, un mai

mare accent trebuie să fie pus pe analiza nodurilor și legăturilor pentru a asigura țintirea cu eficacitate. Scopul afectării nivelului logic este de a interfera cu funcțiile sistem.

Atacurile ar putea include întârzierea executării de proceduri, direcționarea greșită a informației sau infectarea cu viruși software. În cazul afectării ideale, atacatorul nu-i nevoie să distrugă informația sau sistemul ci doar să le controleze. La nivelul cel mai înalt, nivelul semantic, obiectivul atacului este afectarea și/ sau exploatarea încrederii pe care utilizatorul o are în sistemul informațional, în rețea, și în abilitatea lui de a interpreta și a lua decizii pe baza informației. Cadrul nostru larg accentuează faptul că ceea ce militarii numesc Operații Psihologice trebuie să aibă un context mult mai larg în descrierea infrastructurilor informaționale globale sau naționale.

Cadrul larg ce a fost prezentat a încercat să arate cum capacitatea societății de a face față războiului depinde de fiecare componentă a infrastructurii tehnologice care există în prezent. Creșterea continuă a interdependențelor dintre infrastructurile civile și militare, necesită schimbări ale modului în care conflictul este tratat, lansează provocări pentru proiectarea instituțiilor tradiționale și a ierarhiilor și redesenează conceptul de granițe și securitate națională. Așa cum a spus Tedlers, societățile poartă război prin mijloacele lor de a produce bogăție și noi suntem, sau ne deplasăm spre era informațională.

Bazat pe dezvoltarea conceptului inițial, și apoi prin vizite, întâlniri și discuții, Forțele Canadiene au formulat viziunea lor despre Operațiile informaționale (IO). Pentru CF, IO merg dincolo de sistemele informaționale simple și procese, și chiar **IO ar trebui văzute că o STRATEGIE, NU ca pe o capabilitate însăși**.

Dacă este văzută ca o strategie, atunci obiectivul IO devine factorul de decizie, fie că este președinte, prim ministru, comandant sau membru de serviciu individual, marinar, soldat sau aviator. Totuși, IO devine o strategie ce integrează diferite capabilități de realizare a obiectivelor politice și militare. Urmează

)oi că IO include un doneniu larg de capabilități ce ar putea să
ıprindă activități militare - tradiționale cum ar fi distrugerea,
.ducerea în eroare, OPSEC, EW, PSYOPS (C2W) pentru
:tivități bazate pe tehnologie cum ar fi atacuri la rețeaua de
ılculator, sau afaceri civile, afaceri publice și chiar afaceri legale.

Pentru CF, definiția devine: *„Acțiuni desfășurate în sprijinul)biectivelor politice și militare care influențează factorul de decizie ·in afectarea informației și/sau a sistemelor informaționale ale :luilalt simultan cu exploatarea și protejarea propriilor informații /sau sisteme informaționale"*.

Definiția CF pentru IO arăta că informația reprezintă un mijloc factorul de decizie reprezintă finalitatea. Definiția minimizează .tenționat importanța aspectelor tehnice ale IO și se concentrează : toate măsurile ce ar putea fi utilizate pentru a influența factorul : decizie.

În timp ce multe dezbateri au avut loc în Canada, precum și . lume pentru definirea IO, definiția CF a vrut să fie de ansamblu argă). Astfel, ea poate fi aplicată activităților naționale, .ternaționale, civile sau militare și se aplică la fel pentru situații : pace, criză sau război.

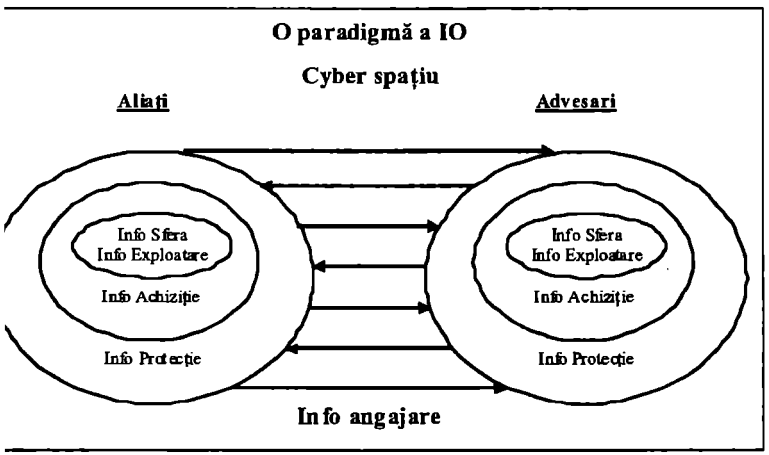


Figura 1: Paradigma operațiilor informaționale (IO).

Paradigma IO care a fost dezvoltată pentru a prezenta mesajul CF și ceea ce a devenit baza pentru dezvoltarea structurii CF au fost o serie de „sfere" de informații așa cum se arăta în figura de mai sus.

Mediul, care a fost numit din lipsa de alte cuvinte mai bune cyber spațiu, conține ansamblul tuturor informațiilor, atât ale adversarilor cât și ale prietenilor. Există patru procese de bază care pot fi realizate în cyber-spațiu: exploatarea informației, achiziția, protecția și intrarea în conflict cu înțelegerea că aceleași activități pot fi desfășurate simultan de oricare adversar.

CF dorește să fie în măsură să exploateze informația de care dispune. Aceasta implică existența unui sistem desemnat să furnizeze informația corespunzătoare utilizatorului corespunzător la momentul potrivit. CF va avea nevoie să achiziționeze informația, cea despre adversarii noștri posibili din diferite surse de intelligence și prin alte mijloace cât și despre aliați și prieteni pentru a asigura compatibilitatea. Oricând se culege sau se exploatează informație, este nevoie de a proteja informația și procesele prin care se culege și se exploatează. Acest proces va include atât protecția față de adversarii noștri, prin detectarea pătrunderii în sistem/calculator și reacția corespunzătoare față de noi înșine, cum ar fi angajații nemulțumiți sau virușii.

Aspectul de protecție include de asemenea posibilitatea de a recupera și de a utiliza echipamentele după pătrunderea neautorizată sau disfuncționalități. În final, CF are nevoie să facă față adversarilor (sau „inamicilor") prin încercarea de a preveni sau limita posibilitatea lor de a achiziționa informații, realizată prin mecanisme de protecție și obținerea sau deținerea controlului informațiilor lor și/sau proceselor.

Rezultă din aceste patru procese și funcții, exploatarea, achiziționarea, protejarea și intrarea în conflict, că CF are dezvoltate structura și activitățile Grupului său de IO pentru a fi în măsură să-și îndeplinească responsabilitățile și mandatele.

Paralel cu acest efort, Departamentul Apărării, a implicat de asemenea alte departamente guvernamentale și Biroul Consiliului

Privat (activități guvernamentale centrale) atât la nivel executiv cât și de conducere, pentru a stabili un răspuns guvernamental coordonat la amenințări și vulnerabilități. DND a înțeles că are un rol important de jucat ca partener în procesul mai larg desfășurat de Guvernul Canadei. Această viziune s-a integrat bine cu conceptul mai larg al Infrastructurilor Informaționale Globale și Naționale, protecția lor și rolul Canadei în cadrul acestor procese.

Inițial CF a stabilit un grup de lucru pentru IO pentru a aborda multe din problemele care erau nevoie să fie investigate pentru ca militarii să devină valoroși în domeniul IO, incluzând conceptele, doctrinele, politicile, cerințele CF și instruirea. Gupul a cuprins componentele majore ale DND (Departamentul Apărării Naționale), incluzând Operații J3, servicii de informații, structuri de servicii, aspecte legale, politici, ofițeri de securitatea informației (CIO) și domeniul afacerilor publice.

Încă de la început, CF a restructurat grupul pentru a forma Grupul de Operații Informaționale al CF (CFIOG). Acest efort a integrat și consolidat multe funcții ce se legau de activitățile de IO pentru a forma o singură voce care să reprezinte activitățile de IO. Au fost stabilite noi activități bazate pe paradigma de IO ce a fost descrisă mai devreme.

O Echipă de Evaluare a Vulnerabilităților Naționale (NVAT) a fost stabilită inițial pentru a începe rolul de protecție a resurselor de informații a CF. Această activitate a fost acum preluată de Echipa de Răspuns la Incidente Calculator (CIRT) și care stabilește în prezent mecanismele pentru detectarea, raportarea și investigarea încercărilor de pătrundere neautorizată în sistemele informaționale ale militarilor.

În paralel cu aceste eforturi, a fost scrisă, aprobată și diseminată doctrina CF. Doctrinele individuale ale serviciilor au fost pregătite și integrate cu cadrul mai larg al Doctrinei CF. Pe măsură ce aceste aspecte au fost completate fără întârzieri majore, dezvoltarea Politicii CF a fost mult mai dificilă. Cele mai ample

probleme au generat preocupări privind rolul și activitatea PSYOPS, legătura acesteia cu Afacerile Publice, și aspecte legale ale activităților IO ofensive și defensive. Unele dintre elementele cheie ale conținutului politicii recent aprobate sunt:

a. IO reprezintă o strategie integrată ce se concentrează pe toate aspectele de influențare a factorilor de decizie.

b. IO nu reprezintă o simplă problemă tehnică, dar include lucruri cum ar fi afacerile (activitățile) publice, PSYOPS și vulnerabilități ale infrastructurii guvernamentale.

c. Comandanții sunt responsabili pentru implementarea IO defensive.

d. Coordonarea IO va fi realizată de către o Celulă de Coordonare a Operațiilor informaționale (IOCC).

Conceptul de IOCC a fost desemnat pentru a furniza intrări de IO pentru planurile dezvoltate de către Statul Major Național. Structura s-a dorit să fie flexibilă, adaptată pentru a îndeplini cerințele specifice. Pe măsură ce conceptul a fost acceptat, el trebuie încă să fie activat consistent în cadrul exercițiilor și operațiilor. Introducerea IO necesită regândirea profundă de către statul major și realinierea preocupărilor pentru toate procesele de planificare. Va fi, fără îndoială, nevoie timp pentru ca aceste considerații să devină un element uzual pentru planificatorii de IO.

De la primele stadii ale dezvoltării conceptului de IO, s-a afirmat clar că este nevoie că reprezentanții comunității de R&D să fie implicați în sprijinirea procesului de IO specific CF. Fiecare dintre procesele de IO definite în paradigma de IO: protecția, exploatarea, achiziția și tratarea adversarului necesită o contribuție importantă a R&D pentru ca CF să-și îndeplinească rolul pe deplin. Acest rol a devenit o provocare particulară în cadrul legăturii realizate între tehnologiile și cerințele militare și civile.

În cadrul CF, J6 a primit rolul de coordonare a dezvoltării IO. Un stat major restrâns de IO formează nucleul permanent cu rol de coordonare a IO și furnizează vizibilitatea necesară IO pentru a implementa schimbări. Acest rol nu include numai

funcțiile CF și ale Guvernului Canadei, ci și legăturile noastre internaționale. Ei au avantajul de a realiza implementarea conceptelor de IO și de a stabili structurile care să corespundă cerințelor.

Conceptul de bază ce a fost stabilit inițial și menținut pe parcursul procesului de dezvoltare al IO a fost că IO reprezintă o strategie care cuprinde un mediu informațional care depășește pe cel specific numai domeniului militar. Această abordare holistică necesită totuși contribuții din partea tuturor pentru a funcționa efectiv, altfel DND operează în vid.

Cea mai mare dificultate înregistrată de DND este probabil reluctanța (nedorința) Guvernului Canadei de a accepta rolul conducător care este necesar în abordarea holistică și un rol în care toți participanții implicați să-l considere ca necesar. Apărarea națională se vede ea însăși ca un element important, dar reprezintă numai un membru cooperativ integrat într-un rol național mai larg.

Altă dificultate ce a apărut în situația Canadei a fost încrederea în încorporarea de dezvoltări de IO și studii ce-și au originea în afara poziției Canadei. Aceasta va diminua rolul Canadei ca un inovator de IO, atât în domeniul militar cât și civil. Totuși, se poate afirma că prin adoptarea unei abordări prudente, Canada va evita greșelile repetate de dinainte, dar la un cost de pierdere a unicității ei, care ar putea fi stabilit. Totuși, în acest proces, DND este gata să meargă mai departe pe arena IO fără avantajul unei conduceri centrale puternice.

Nu este totuși surprinzător, că rămâne numai Canada una dintre țările vestice/ avansate tehnologic a cărui guvern nu a sponsorizat existența unei echipe de răspuns la incidentele calculator. În cadrul abordării holistice adoptate de DND, conceptul de informație ca bun național reprezintă o premisă fundamentală și ca rezultat necesită să fie luate în considerare măsuri de securitate națională corespunzătoare.

În mod sigur un avantaj al abordării holistice a fost dezvoltarea relativ uniformă a politicii și doctrinei DND. În particular,

integrarea politicilor și doctrinelor individuale ale serviciilor a fost făcută mai ușor. Încercarea de a realiza un consens departamental, lăsând deoparte consensul național, este mult mai dificilă dacă aceasta este condusă de jos în sus.

Introducerea IO în Departament a creat oportunitatea pentru stabilirea de noi roluri, în special în unele locuri tradiționale. De exemplu, pentru J6 care era tradițional responsabilă pentru sprijin de comunicații și sprijin electronic s-a găsit ea însași în măsură să controleze „arme operaționale" în forma calculatoarelor și rețelelor. În timp ce J6 în Canada a crezut ferm în rolul său de conducere a elementelor operaționale ale departamentului ce revin domeniului IO, lor au trebuit să le fie date responsabilități în domenii ce nu erau tradițional în mandatul lor.

Deoarece tranziția înceată înspre Grupul de IO a avut loc, a fost evident că un număr de roluri și structuri tradiționale urmau să fie schimbate. A fost o caracteristică a multor organizații, nu numai a DND dar peste tot la fel, a existat tendința de a consolida și proteja structurile și funcțiile existente. Chiar cu o abordare holistică pentru IO, și în dezvoltarea organizațională în general, mai curând decât să se opereze intern și protectiv, este mai benefic să se îmbunătățească competențele și funcțiile. Aceasta este o lecție dificil de învățat.

Cu noul concept IO, este de asemenea necesar să fie pregătit personal cu un nou set de capabilități și să fie plasat în roluri noi, netradiționale. Înseamnă că trebuie create noi oportunități de instruire, și în cadrul sistemului de personal, recunoașterea rolurilor noi și a responsabilităților ce sunt asociate cu îndeplinirea funcțiilor legate de IO.

Abordarea holistică a făcut aceste oportunități să se dezvolte mai încet decât rolurile tradiționale, și instruirea primește încă cea mai mare atenție și sprijin. Personalul militar nu mai poate să aștepte să fie numit într-o nouă poziție pentru trei ani și apoi să se mute. Instruirea și cerințele pentru lucrul în cadrul IO necesită o implicare mai lungă și o instruire permanentă, pentru a rămâne în

top. Aceste probleme necesită încă rafinare în cadrul CF pentru a beneficia din plin de programul de IO.

Comunitatea militară de R&D s-a aflat într-o poziție dificilă. În primul rând ea trebuia să se lupte cu resursele guvernamentale reduse. În al doilea rând, și mai important, ea trebuia să facă față competitorilor civili/comerciali ce se aflau în topul tehnologic de un număr de ani.

Aceasta însemna de asemenea că rolul tradițional al R&D trebuia să se schimbe sau să se adapteze la a fi un integrator de top mai curând decât a fi un inovator. Aceasta este relevant în special în situația Canadei care produce adesea sisteme complete dar mai frecvent furnizează componente sau produce sisteme hibride ce integrează tehnologii și concepte numeroase. La fel pentru a menține pacea cu sectoarele civile și comerciale, conceptele anterioare de cercetare pe termen lung, mediu și scurt au trebuit să fie regândite.

Din cauza creșterii integrării necesare, este aproape o necesitate pentru oamenii de știință R&D să lucreze mână în mână cu operatorul pentru a fi integrat deplin în strategia operațională de IO.

De la grupurile de lucru inițiale de IO, a fost mai mult decât clar că noi alocări financiare ar putea fi așteptate pentru activitați de IO. S-a așteptat ca fondurile existente să fie re-alocate pentru a face față nevoilor. Într-o abordare holistică, oportunitățile de a găsi fondurile realocate sunt dificile, deoarece fiecare organizație și fiecare manager va încerca să-și protejeze resursele limitate.

Chiar abordarea SUA de a lucra cu elementele serviciilor individuale duce eventual la un punct unde nu există pe mai departe oportunitatea de a realoca sau ajusta fonduri. Deoarece IO a fost introdus ca un nou concept cu propriul său set de amenințări și vulnerabilitați, a devenit necesară injectarea de noi fonduri și personal în acest domeniu.

RĂZBOIUL INFORMAȚIONAL PROBLEME DE SECURITATE

Dr. W. STEIN*

Scopul acestei lucrări este de a găsi orientările, ilustrațiile utile, precum și definițiile, și poate factorii critici care pot ajuta la deschiderea unei porți pentru cooperarea mai bună în domeniul cercetării, dezvoltării și educației corespunzătoare problemelor prezente legate de securitatea informației. Acest domeniu include Securitatea Informației (INFOSEC),

Războiul informațional (IW) și Protecția Infrastructurii Critice (CIP). Se pot găsi mulți factori tradiționali ce influențează înțelegerea și cooperarea ce pot să includă termeni și definiții diferite, competiția economică, și interese de securitate națională. Rezultă că există un domeniu de probleme comune în contextul războiului informațional, cu provocări pentru un nou nivel de cooperare în știință, inginerie și educație.

A fost acceptat în timp că sectorul de informații și comunicații cu sistemele și infrastructurile lor informaționale reprezintă un element central al tuturor celelalte sectoare ale societăților moderne, necesare pentru funcționarea de bază a fiecărui aspect național și internațional. Atacurile asupra sistemelor informaționale reprezintă deja un fapt cotidian al erei informaționale.

Aproape zilnic, hackerii exploatează vulnerabilitățile din infrastructura noastră informațională globală și din sistemele de calcul. Diferiți adversari ideologici și culturali - individual, grupuri de guerrilă și grupuri teroriste - sunt pe cale să descopere „Războiul

* Armata Germană.

informațional" ca un mijloc major de afectare a activităților din sectorul guvernamental, militar și cel al corporațiilor. Guvernele, forțele armate și societatea ca un întreg, au nevoie de a fi pregătiți în scopul de a face față acestor amenințări și atacuri informaționale. Dar în mod curent se pare că există o lipsă de conștientizare privind securitatea informațională și vulnerabilitățile infrastructurilor.

Deși o categorie redusă din aceste atacuri se concretizează în pierderi sau pagube semnificative, marea lor majoritate se concretizează în pagube mici sau inexistente, echivalentul infracțional al pătrunderii neautorizate, deranjarea liniștii publice, vandalism minor, și chiar furt.

A fost estimat că mai mult de 90% din aceste atacuri se desfășoară utilizând unelte și tehnici disponibile (pe baza incidentelor raportate de CERT), că numai un atac din 20 este conștientizat de către o victimă, și numai 1 atac din 20 este raportat (aceste ultime două statistici sunt un rezultat al studiului desfășurat de Agenția Sistemelor Informaționale ale Apărării) și rate similare au fost raportate de către alții). Totuși, se pare că ratele de raportare sunt în creștere. Și așa cum se poate vedea, nu există (aproape) nimic nou în acest domeniu.

Ca o consecință, interesul pentru securitatea informațiilor, calculatoarelor și rețelelor a apărut devreme și primul raport datează din 1970. După apariția programului de Protecție a Infrastructurii Critice (CIP) pe parcursul ultimilor 5–10 ani, noi ne confruntăm acum cu trei domenii referitoare la securitate cu provocări aflate în legătură: Securitatea Informației (INFOSEC), Războiul Informațional (IW) și Protecția Infrastructurii Critice (CIP). Când analizăm problemele referitoare la securitate, putem să găsim diferiți termeni, uneori definiții redundante și domenii care se suprapun (diferit între comunități, națiuni, etc.), de exemplu securitate, siguranță, și protecția și/sau infrastructurilor precum și război informațional și operații informaționale.

Aceste componente eterogene și diverse pot face cooperarea dificilă sau chiar imposibilă. Figura 1 evidențiază domeniile de

Război Informațional (IW), Securitatea Informației (INFOSEC), și Protecția Infrastructurii Critice (CIP) precum și posibilele lor subdomenii aflate în legătură. Deși cele trei domenii au multe subiecte comune (ex., metode, instrumente, în parte utilizând aceleași infrastructuri, având obiective de cercetare și dezvoltare similare, utilizând cadre de lucru pentru analiză similare), gradul de cooperare în cercetare și dezvoltare pare să fie foarte limitat.

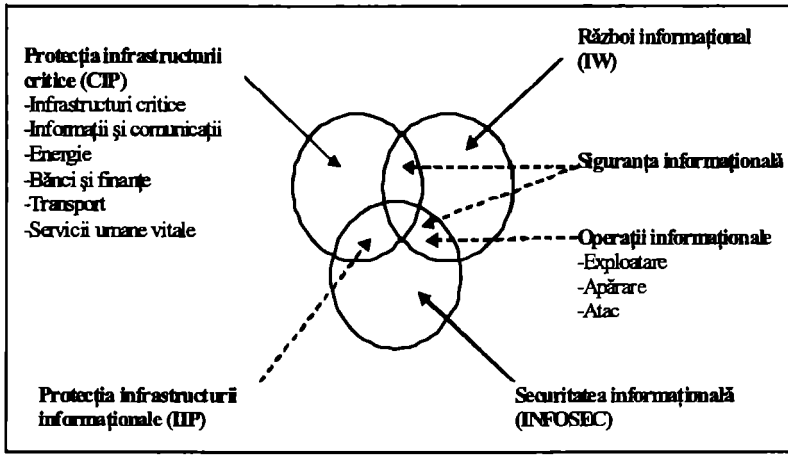


Figura 1. Domenii și subdomenii ale războiului informațional, securității informaționale și protecției infrastructurii critice

Termenul de „securitate informațională" (INFOSEC) este în uz de aproape două sau trei decenii. Standardul federal al SUA îl definește ca *„Protecția informației împotriva dezvăluirii, transferului, modificării, sau sustragerii neautorizate făcută accidental sau intenționat."* Prin contrast, termenul de „siguranță informațională" este relativ nou. În 1996 directiva Departamentului Apărării SUA îl definește ca *„Operații informaționale ce protejează și apără informațiile și sistemele informaționale prin asigurarea disponibilității, integrității, autenticității, confidențialității și non-repudierii lor. Aceasta include suport pentru restaurarea sistemelor informaționale prin încorporarea*

capabilităților de protecție, detecție, și capabilități de reacție." Războiul informațional defensiv este legat îndeaproape de ambele concepte, dar se preocupă numai de atacurile intenționate. Securitatea informațională și siguranța informațională abordează de asemenea amenințări neintenționate, ex. erori, accidente, și dezastre naturale.

Astfel, siguranța informațională este bazată pe definiția operațiilor informaționale și are un înteles oarecum mai larg decât securitatea informațională. Termenul de siguranță informațională poate fi întâlnit în diferite domenii guvernamentale, ex. Departamentul Apărării,

Protecția Infrastructurilor Critice și Agenția de Securitate Națională. NATO definește operațiile informaționale ca *„Acțiuni desfășurate pentru a influența factorii de decizie în sprijinul îndeplinirii obiectivelor militare și politice, prin afectarea informațiilor altora, proceselor bazate pe informații, sisteme de comandă și control, simultan cu exploatarea și protejarea propriei informații și/sau sistemelor informaționale".*

Există două categorii principale ale Info Ops: Info Ops defensive și Info Ops ofensive, depinzând de natura acțiunilor implicate.

Așa cum indică figura 2, provocarea curentă este pentru securizarea sistemelor informaționale conectate în rețea atât din mediul militar cât și civil. Consecvent Organizația de Securitate a Sistemelor Informaționale din cadrul NSA a definit un sistem informațional (IS) ca:

„Întreaga infrastructură, organizare, personal și componente pentru culegerea, prelucrarea, stocarea, transmiterea, afișarea, diseminarea și eliberarea de informații" și securitatea sistemelor informaționale (ISS) ca: *„Protecția sistemelor informaționale împotriva accesului neautorizat sau modificării informației în etapa stocării, prelucrării sau tranzitului, și împotriva interzicerii serviciului pentru utilizatorii autorizați, incluzând acele măsuri necesare pentru detectarea, documentarea și contorizarea a astfel de amenințări".*

Securizarea sistemelor informaționale conectate în rețea necesită o perspectivă acoperitoare asupra sistemului. Securitatea este îndeaproape legată de siguranță și încredere și nu trebuie ignorată sau atribuită preocupărilor incidentale. Noi abordăm aici o vedere mai largă a problemelor ce țin de securitate și siguranță, și considerăm aceste probleme ca o problemă globală unificată la nivelul sistemului/ rețelei/ agenției.

Procedura de securizare indicată în figura 2, poate fi aplicată unui singur calculator, precum și sistemelor și infrastructurilor de IT la nivel național.

Vulnerabilitățile sistemelor (figura 2) sunt omniprezente. Cele mai multe sisteme de operare au un sistem de autentificare slab și sunt ușor de penetrat. Cele mai multe din aceste sisteme au elemente de control al accesului slabe și tind să fie configurate defectuos și ca rezultat există cu ușurință posibilitatea utilizării greșite odată ce este obținut accesul inițial.

Aceste sisteme au adesea facilități de monitorizare care sunt adaptate greșit, pentru a determina când au loc amenințările și ce pericole pot să apără. Uneori, utilizarea greșită de către cei din afară și din interior este posibil să se realizeze și uneori foarte dificil de detectat.

Amenințările la securitate (figura 2) sunt omniprezente. Domeniul amenințărilor ce pot exploata aceste vulnerabilități este enorm, plecând de la activități teroriste posibile, sabotaj, spionaj, competiție industrială sau națională, reproducere neautorizată, funcționări mecanice defectuoase și erori umane.

Atacurile pot implica inserări de Cai Troieni, sau intervenții fizice, incluzând acțiuni plătite de angajați nemulțumiți sau acțiuni de persecuție. Atacurile de interzicere a serviciului sunt insidioase în particular, deoarece este dificil de a realiza apărarea împotriva lor și efectele lor pot fi devastatoare. Sistemele conectate la Internet sau disponibile prin linii de conexiune sunt victime posibile ale pătrunderilor externe.

Chiar sistemele ce par să fie complet izolate sunt subiect de

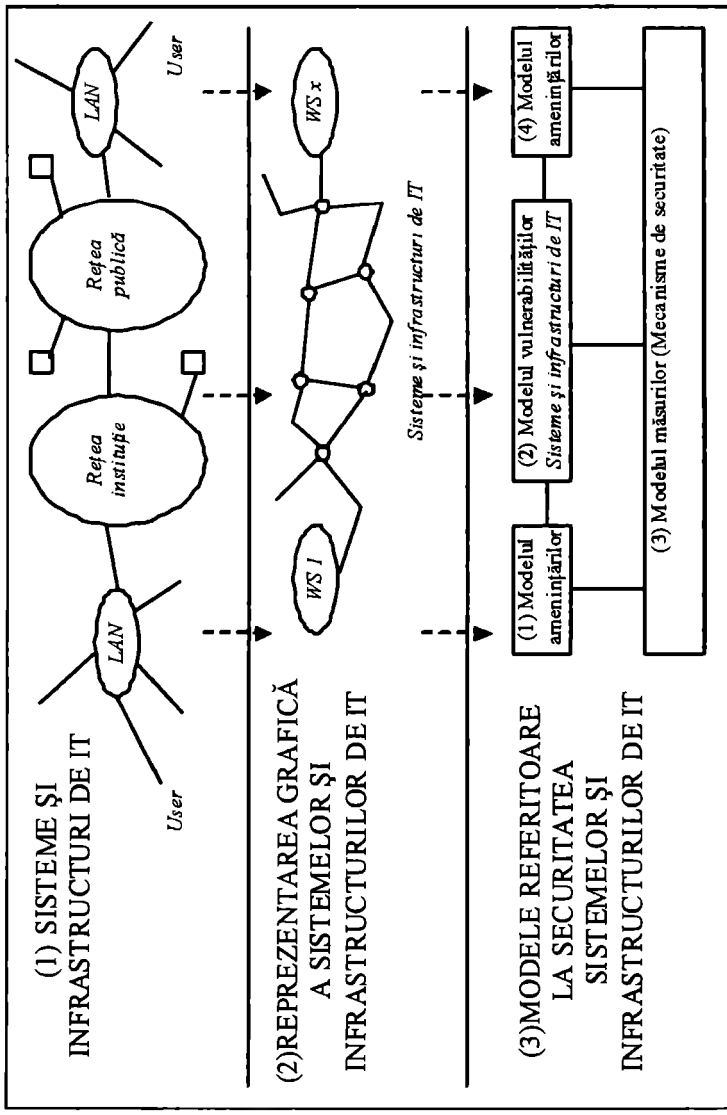


Figura 2. Pași în securizarea sistemelor informaționale: analiza vulnerabilităților, amenințărlor și riscurilor

utilizare internă greșită. Suplimentar, multe din aceste sisteme ce par izolate pot fi compromise prin acțiune de la distanță din cauza facilităților lor de diagnosticare și mentenanță de la distanță.

Riscurile sunt omniprezente (figura 2). Consecințele acestor vulnerabilități și a amenințărilor asociate denotă că riscurile pot fi considerabile. Utilizarea greșită a calculatoarelor poate avea ca rezultat (de exemplu pierderea de confidențialitate: pierderea integrității sistemului atunci când sistemele sunt afectate, pierderea integrității datelor atunci când datele sunt alterate, interzicerea serviciului ce fac resursele furnizate nedisponibile, sau chiar furturi de servicii).

Securitatea informațională (INFOSEC) este fundamentală și sub unele aspecte reprezintă chiar o parte clasică a celor trei probleme referitoare la securitate. Securitatea informațională (sau securitatea calculatoarelor, cum a fost ea numită inițial), a fost pentru prima dată prezentată într-o formă completă într-un raport din anul 1970 al Biroului de Știință al Apărării, dar experiența practică și operațională, în particular încorporarea măsurilor de securitate în cadrul sistemelor, a avut loc mult mai târziu.

Securitatea calculatoarelor ca disciplină a fost studiată pentru prima dată la începutul anilor 1970 deși problemele referitoare la aceasta au influențat dezvoltarea anterioară a multor sisteme. Deceniul anilor 1970 a fost caracterizat de cercetările finanțate de Departamentul Apărării, în special de către Forțele Aeriene și DARPA. Experiența celorlalte națiuni (lumii întregi) nu s-a manifestat până la publicarea lucrării „Criterii de evaluare a încrederii în sistemele de calcul specifice Departamentului Apărării", cunoscută sub denumirea de „Cartea Portocalie" sau TCSEC.

De-a lungul anilor 1970 și 1980, eforturile INFOSEC s-au concentrat pe criterii de evaluare a încrederii în securitatea calculatoarelor neconectate în rețea (TCSEC) și securitatea comunicațiilor (COMSEC) pentru comunicații militare și

naționale. Chiar și așa, sisteme care încorporează măsuri de securitate nu au fost instalate până în ultima parte a anilor 1980.

Subiectul operațiilor informaționale a fost dezvoltat în experimente de către forțele SUA, în special între anii 1985-1995. Începând cu ultima parte a anilor 1980 a existat un interes sporit în protejarea infrastructurilor critice de care societatea depinde pentru a face față atacurilor fizice și informaționale. Institutul Tehnologiilor Critice (condus de RAND) a fost creat în 1991 pe baza unei hotărâri a Congresului și a studiat și definit probleme referitoare la Protecția Infrastructurilor Critice (CIP).

Intuitiv, înțelesul în limbajul natural al securității implică protecția împotriva evenimentelor nedorite. Securitatea sistemului și securitatea datelor sunt două tipuri de securitate. INFOSEC poate fi definită la două nivele. La nivel politic, INFOSEC reprezintă sistemul de politici, proceduri și cerințe de protecție a informației; la nivel tehnic, INFOSEC include măsuri și controale ce protejează infrastructura informațională împotriva interzicerii serviciului, pătrunderii neautorizate, și modificării sau distrugerii componentelor infrastructurii informaționale (inclusiv date). INFOSEC include totalitatea măsurilor de securitate necesare pentru a furniza un nivel de protecție acceptabil pentru o infrastructură și pentru datele vehiculate de o infrastructură.

Mai recent, aspectul de supraviețuire (capacitatea de a face față atacurilor, și de asigurare a funcționalității la un anumit nivel de performanță) a fost recunoscut că o componentă critică a apărării.

Este de dorit un sistem de ansamblu și un set de cerințe reale referitoare la conectarea largă în rețea, care presupun securitatea, încrederea, toleranța la defectări, performanța, și orice alte atribute necesare pentru păstrarea unui sistem adecvat și a supraviețuirii în rețea. Subiectul cel mai general al cerințelor de securitate este dependabilitatea (în unele lucrari abordată că supraviețuire). Dependabilitatea (sau supraviețuirea) include cerințe pentru componente (A) securitatea, (B) încrederea și (C) performanța.

Proprietățile de bază ale securității sunt (1) confidențialitatea, (2) integritatea, și (3) disponibilitatea. Supraviețuirea este capacitatea unui sistem informațional conectat în rețea de a satisface și de a continua să satisfacă cerințe critice certe (ex. cerințe pentru securitate, încredere, răspuns în timp real, și corectitudine) în fața condițiilor adversarului. Supraviețuirea trebuie să fie definită cu privire la setul de adversități ce sunt presupuse că pot să existe.

Tipurile de adversități pot să includă în mod obișnuit defecte hardware, defecte soft, atacuri asupra sistemelor și rețelelor care conțin utilizatori necorespunzători, și interferențe electromagnetice. Deoarece este adesea făcută pentru încredere, supraviețuirea ar putea fi definită alternativ că o măsură probabilistică a cât de bine sunt satisfăcute anumite cerințe date. Dar, de cele mai multe ori, este preferată o definiție ne-cantitativă.

Există legături clare între conceptul de supraviețuire și dependabilitate a sistemului. Cele trei atribute de bază ale securității sunt (1-3), și sunt utilizate și alte trei atribute suplimentare (4-6).

1. confidențialitatea protejează existența unei conexiuni, fluxul traficului, și informația împotriva dezvăluirii.

2. Integritatea asigură că informația și procesele sunt sigure împotriva accesului neautorizat prin metode cum ar fi criptarea, semnături digitale, și detectarea pătrunderii.

3. Disponibilitatea furnizează asigurarea că informația și serviciile vor fi accesibile și utilizabile atunci când este nevoie.

4. Autenticitatea asigură că numai utilizatori autorizați au acces la informații și servicii.

5. Ne-repudierea asigură că tranzacțiile sunt imune împotriva refuzului fals al trimiterii sau recepționării de informații prin furnizarea unei evidențe de încredere ce poate fi verificată independent pentru a stabili profilul originii și livrării.

6. Restaurarea asigură că informația și sistemele pot supraviețui unui atac și că disponibilitatea poate fi refăcută după impactul unui atac.

Securitatea include atât securitatea sistemelor cât și securitatea informației. Trebuiesc anticipate toate amenințările reale, incluzând utilizarea greșită de către utilizatorii din interior, penetrări de către utilizatorii din afară, interferența accidentală sau intenționată (ex. electromagnetic), emanații, canale ascunse, inferență, și agregări. Pentru a asigura securitatea este nevoie de mai mult decât de confidențialitate, integritate și disponibilitate.

Este nevoie de încredere, definită în general ca o măsură a cât de bine operează un sistem în cadrul specificațiilor lui. De exemplu, toleranța la defectări poate activa o varietate de alternative, incluzând moduri de operare în timp real, pierderea siguranței, pierdere ușoară, pierdere rapidă și pierderea securității. Performanța este o cerință critică. În unele cazuri, performanța adecvată poate fi critică pentru supraviețuirea unui sistem sau a unei aplicații.

Pe de alt parte, în cele mai multe cazuri, performanța este ea însăși dependentă de supraviețuire și disponibilitate. Dacă un sistem nu supraviețuiește, performanța adecvată nu poate fi realizată. Ce este evident imediat este că există legături strânse între diferite cerințe.

Aici au fost rezumați pașii de securizare a sistemelor informaționale conectate în rețea (figura 2) așa cum au fost descriși de Waltz. Analizele de securitate trebuie să fie aplicate pentru a determina gradul de risc al sistemului, pentru a identifica proiectarea, configurația, și alte defecte și vulnerabilități, și pentru a verifica concordanța cu politica și modelul cerințelor de securitate. Analizele pot să varieze de la o evaluare informală la o analiză de ansamblu și exhaustivă.

Primul pas în procesul de analiză include o evaluare a amenințărilor la adresa sistemului, bazată pe informații și extrapolări ale capabilităților tehnologice. Evaluarea de vulnerabilitate presupune domeniile de acces posibil (intern și extern) și are în vedere vulnerabilitatea relativă (sau punctele slabe de securitate) corespunzătoare atacului. Vulnerabilitățile pot fi

atribuite eșecurilor în analiza, proiectarea, implementarea, sau operarea unei rețele sau sistem.

Rezultatul evaluărilor amenințărilor și vulnerabilităților este o matrice a amenințărilor ce clasifică amenințările (prin categoria de atac) și vulnerabilitățile (prin funcții). Matricea furnizează o ierarhizare relativă a probabilității amenințărilor și a impactului posibil ale atacurilor adverse asupra fiecărei zone de vulnerabilitate. Aceste date formează baza pentru evaluarea de risc.

Procesul de management al riscului începe cu evaluarea riscurilor la sistemul care are asociată o matrice a riscurilor. Riscurile sunt cuantificate în termeni de probabilitate a apariției și a gradului de impact nedorit dacă apariția are loc. Pe baza acestei ierarhizări a riscurilor, este dezvoltată o abordare a managementului de risc ce îndeplinește cerințele de securitate ale sistemului.

Securitatea poate fi cuantificată în termeni de risc, și include patru componente: (1) procentul atacurilor detectate; (2) procentul detectat și controlat; (3) procentul detectat, controlat și recuperat și (4) procentul de risc rezidual. Aceste faze introduc trei alternative de management de risc.

(1) Riscul acceptat: Dacă amenințarea este puțin probabilă și impactul advers este nesemnificativ, riscul poate fi acceptat și nu sunt impuse în continuare cerințe de securitate suplimentare.

(2) Risc tratat (sau administrat): Dacă riscul este moderat, măsurile pot fi luate pentru a minimiza probabilitatea apariției sau a impactului nedorit sau a amândorura. Aceste măsuri pot să includă o combinație de OPSEC, TCSEC, INFOSEC, sau cerințe interne de proiectare, dar efectul combinat trebuie să fie analizat pentru a obține reducerea dorită a riscurilor în scopul îndeplinirii cerințelor de sistem de nivel înalt.

(3) Risc evitat: Pentru riscurile cele mai drastice, caracterizate de probabilitate ridicată de atac sau de impact nedorit accentuat, sau de ambele, poate fi aleasă o abordare de evitare a riscului. Aici, sunt aplicate cele mai ridicate nivele ale proceselor de tratare

a riscului (măsuri de securitate de înalt nivel) pentru a obține o probabilitate suficient de scăzută la care riscul poate să aibă loc în operarea sistemului.

Când amenințările și vulnerabilitățile sunt înțelese, riscurile cuantificate și măsurate sunt aplicate pentru a controla balanța de risc, pentru a îndeplini util cerințele de securitate de nivel înalt și astfel administrarea în ansamblu a riscului sistem. Etapa de proiectare, apoi implementările proiectării, trebuie să fie subiect a analizelor de proiectare și a testării pentru verificarea securității.

Suplimentar, o echipă roșie independentă poate fi aleasă pentru a conduce atacurile simulate asupra sistemului și pentru a evalua performanța de securitate actuală. Atacurile echipelor roșii (numite frecvent „teste de penetrare") vizează securitatea fizică și operațională precum și aspectele tehnice ale sistemului. Rezultatul verificarilor echipei roșii poate să se concretizeze în modificari de proiectare pentru a asigura corespondența cu cerințele de securitate sistem.

La fel ca și la securitatea și siguranța informațională, trebuie să ne gândim mai întai la definiții și înțeles, deoarece războiul informațional înseamnă un număr de lucruri diferite - probabil o combinație a tuturor acestora și ceea ce înseamnă cu adevărat depinde de tendința particulară a cuiva. (1) Luptătorii informaționali puri văd războiul informațional ca un război fără bombe sau gloanțe; un conflict de orice magnitudine dus oriunde, independent de motivație. (2) Următorul grup crede în războiul informațional. Mulți dintre acești oameni simt că posibilitățile de luptă în război pot fi sporite prin aportul tehnologiilor informaționale mai bune. (3) Războiul bazat pe cunoștințe reprezintă o extrapolare inteligentă în devenire a ultimului concept și face o distincție între informație și valoarea crescută subiectiv a cunoștințelor. În cele din urmă, războiul informațional reprezintă o convergență a problemelor de securitate militare și civile și a modului cum oamenii le tratează într-o lume în rapidă schimbare.

Obiectivul războiului bazat pe informații este în final realizarea de scopuri militare cu aplicarea cea mai eficientă a resurselor de informații. Operațiile informaționale ofensive sunt acte ce conduc la îndeplinirea obiectivelor strategice, operaționale sau tactice ale corpurilor guvernamentale autorizate; organizațiilor legale, criminale sau teroriste, corporațiilor, sau ale indivizilor.

Atacurile informaționale ofensive au două funcții de bază: culegerea, respectiv afectarea informației. Superioritatea informațională reprezintă capabilitatea de a colecta, prelucra și disemina un flux neîntrerupt de informații simultan cu exploatarea sau interzicerea posibilității adversarului să facă la fel. Dacă operațiile informaționale sunt realizate în contextul unei strategii, ele au un obiectiv dorit (sau stat final) ce poate fi obținut prin influențarea unei ținte (obiectul influenței).

Operațiile informaționale sunt definite de către Armata SUA ca operații militare continue în cadrul Mediului Informațional Militar (MIE) ce activează, îmbunătățesc și protejează capacitatea forțelor prietene de a colecta, prelucra, și, utiliza informația pentru a obține un avantaj în cadrul întregului domeniu al operațiilor militare. Operațiile informaționale includ interacțiunea cu Mediul Informațional Global (GIE) și exploatarea sau interzicerea informațiilor și capabilităților de decizie ale unui adversar.

Un model funcțional simplu este prezentat (figura 3) pentru a forma baza pentru discuții viitoare ale operațiilor și tehnicilor angajate. Modelul este o extensie a modelului de conflict de bază și include concepte ce evidențiază trei domenii conceptuale ale activității de operații informaționale.

Modelul evidențiază că țintele există în (1) spațiul fizic, (2) cyber-spațiu, și (3) mintea oamenilor. Ținta de nivelul cel mai înalt al operațiilor informaționale este percepția umană a factorilor de decizie, oamenilor politici, comandanților militari și chiar a întregii populații. Țintele finale și obiectivul operațional este influențarea percepției lor privind deciziile și activitățile rezultate.

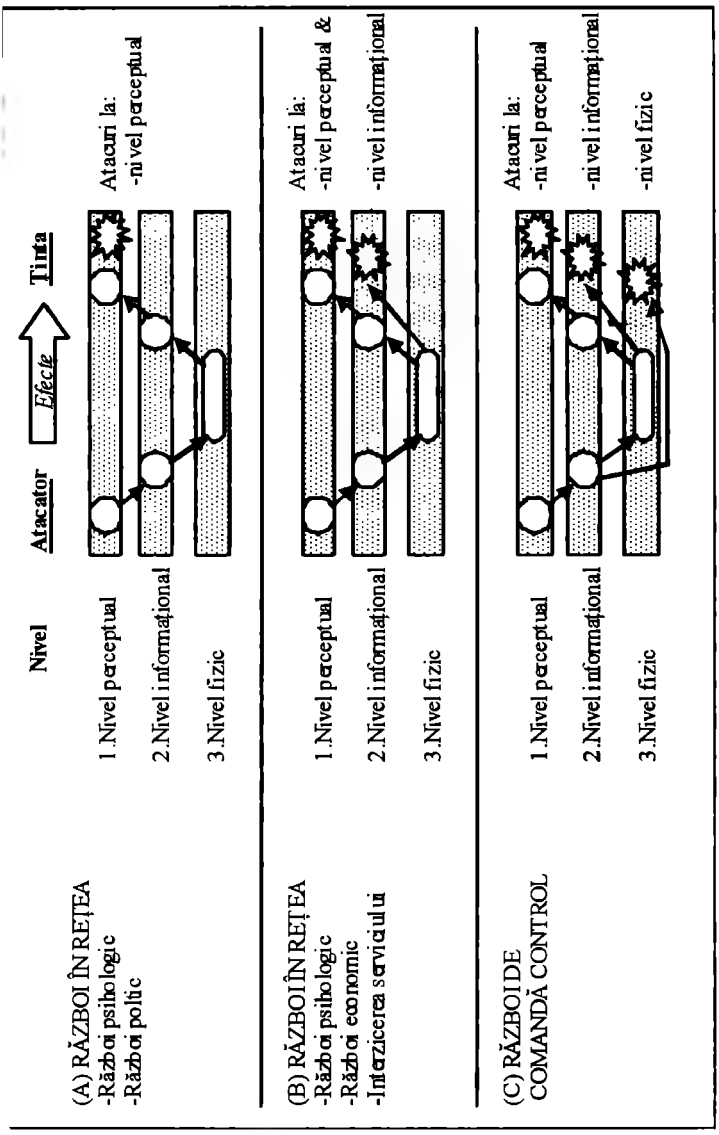


Figura 3: Modelul pe trei nivele al operațiilor informaționale

Modelul operațiilor informaționale (figura 3) distinge trei nivele sau straturi atât pe partea atacatorului cât și pe cea a țintei. Straturile sunt ierarhice, cu influență de sus în jos pentru atacator și cu influență de jos în sus pentru țintă. Obiectivul atacatorului este să influențeze ținta la nivel perceptual prin acțiuni ce pot avea loc la toate nivelurile ierarhiei. Cele trei nivele respectă modelul cognitiv, care conține cunoștințe la nivelul cel mai înalt, informații la nivelul intermediar și date la nivelul cel mai de jos.

Primul strat este la nivel perceptiv sau psihologic, care este de natură abstractă și este orientat spre managementul percepției, pentru ținta vizată. La acest nivel, obiectivul strategic definește acțiunile dorite ale țintei și percepțiile care vor determina cel mai probabil aceste acțiuni.

Dacă acțiunea dorită este determinarea agresiunii, de exemplu, percepția obiectiv pentru conducătorii țintă poate fi *„ajungerea la pierderea controlului, dezordine și pierderea suportului populației"*. Dacă acțiunea dorită este neimplicarea într-o acțiune militară, percepția obiectiv pentru comandanții militari poate fi *„lipsa de suport logistic pentru susținerea operației"*. Aceste percepții obiectiv pot fi realizate printr-o varietate de mijloace fizice sau abstracte (informaționale), dar ținta și obiectivul final este numai la nivel perceptual abstract și efectele influențează comportamentul operațional.

Al doilea strat este stratul infrastructurii informaționale care include infrastructura informațională abstractă care acceptă, prelucrează, administrează și stochează informația. Acesta este stratul care este considerat cel mai adesea că fiind dimensiunea de „cyberspațiu" în care pot avea loc atacuri cu software daunător și atacuri de exploatare a infrastructurii (hacking). Atacurile pe acest strat intermediar pot avea efecte specifice sau în cascadă asupra straturilor perceptuale și fizice.

Al treilea strat este nivelul fizic al sistemului, care include calculatoarele, rețelele fizice, telecomunicațiile și componentele structurale de sprijin (ex. tensiune, facilități, controlul mediului

de lucru) ce implementează sistemul informațional. De asemenea, la acest nivel se află administratorii umani ai sistemelor a căror influență fizică asupra sistemelor este determinantă. Atacurile la acest nivel sunt de natura fizică.

Atacurile pot să aibă loc direct asupra stratului perceptual (ex. întâlniri directe dintre lideri în care discursul uman este utilizat pentru a influența percepția unei ținte sau pentru a colecta informații) sau ele pot viza starturile de jos cu intenția de a avea în consecință influențe pe alte straturi.

Modelul ilustrează cum trebuiesc considerate elementele operaționale la fiecare nivel al modelului. Să considerăm, de exemplu, cum trebuie considerată culegerea de informații pentru indicare și avertisment, țintire și evaluarea pagubelor în luptă pe toate cele trei nivele.

În figura 3, sunt ilustrate amenințările de atac prin modelul războiului informațional pentru trei categorii de război informațional. Exploatarea straturilor fizic și informațional, numai pentru scopuri de management al percepției sau război psihologic (PSYWAR), este ilustrată în partea de sus a figurii. Războiul de comandă și control (C2W), în care atacurile au loc la toate trei nivelurile, este reprezentat în partea de jos a figurii.

Aceste distincții sunt reprezentative numai prin acceptarea că în conflictele reale, atacurile vor avea loc pe toate nivelurile cu diferite grade de intensitate. Rețeaua de război la scară largă, de exemplu, poate fi susținută de elemente la scară redusă dar cu atacuri fizice cruciale asupra infrastructurii sau personalului pentru a îndeplini obiectivele de ansamblu.

Pe parcursul ultimilor cinci la zece ani, a crescut interesul pentru protejarea infrastructurilor critice de care societatea depinde pentru a face față atacurilor fizice și informaționale. Organizația pentru Securitatea Sistemelor Informaționale a NSA (NSA/ISSO) definește: *„Infrastructurile critice sunt acele sisteme fizice și sisteme bazate pe IT (tehnologia informației) esențiale pentru operațiile minime ale economiei și guvernului."*

Trebuie să considerăm diferite tipuri de infrastructuri: (1) infrastructuri critice naționale, (2) infrastructuri informaționale cum ar fi rețeaua Internet - sau orice poate s-o înlocuiască - o Infrastructură Informațională Națională (NII), sau o Infrastructură Informațională Globală (GII) -și (3) software existent pe sistemele de calcul și software de rețea. Este important din perspectiva prezentă acceptarea că există vulnerabilități și amenințări serioase asupra acestor infrastructuri critice. Poate la fel de important este acceptarea că aceste infrastructuri critice sunt interdependente îndeaproape și că ele toate depind de infrastructurile de comunicație-calculator existente.

Pentru o anumită țară, un set caracteristic de sectoare cu infrastructură critică pot fi găsite prin indentificarea atributelor țării, structurii sale, organizațiilor și instituțiilor sale care contribuie inerent la bunăstare, și determină o estimare a nivelului prezent de bunăstare.

Potrivit viziunii SUA, aceste infrastructuri subsumează inițial opt sectoare majore: informații și comunicații, energie electrică, finanțe și bănci, apă și canalizare, transport, petrol și gaz, servicii de urgență (ex. poliție, incendiu, medical) și servicii guvernamentale de bază. Pe baza lucrărilor comisiilor, revizuirii, modificarilor ușoare și agregării aceste sectoare au devenit cinci: (1) Informații și comunicații; (2) Energie; (3) Bănci și Finanțe; (4) Transport și (5) Servicii Umane Vitale. Multe dintre aceste infrastructuri critice au devenit tot mai mult internaționale. Aceasta este o consecință logică a creșterii globalizării.

Conceptul unei infrastructuri informaționale de bază minimale (MEII) se referă la supraviețuirea și asigurarea disponibilității unor infrastructuri informaționale de bază, în special pentru a face față formelor diferite de atacuri de război informațional. Conceptul a fost propus în comunitatea infrastructurilor critice pentru a asigura că unele funcționalități de bază ar putea să existe continuu în contextul unui domeniu rezonabil al amenințărilor privind supraviețuirea - atacuri, îmbătrânire, eșecuri, disturbanțe de mediu și așa mai departe.

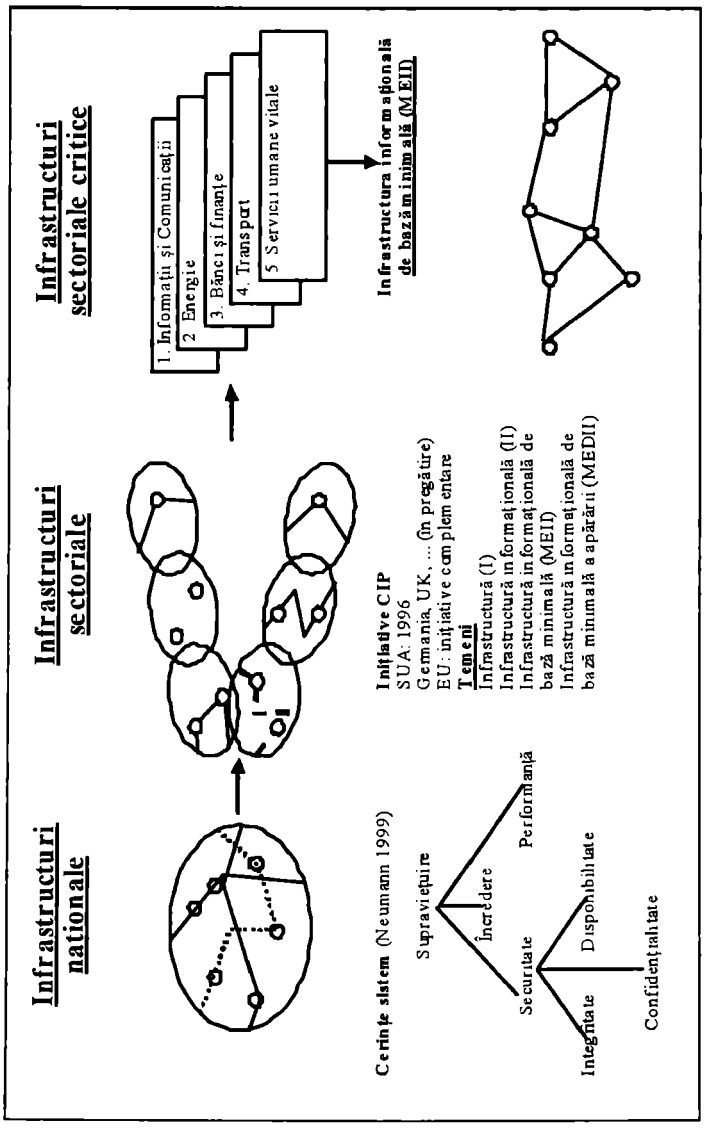


Figura 4: Abordare pentru protecția infrastructurii critice

Până acum există o dezbatere considerabilă asupra definițiilor de minimal și de bază - precum și asupra recunoașterii problemelor inerente în încercarea de a concentra o singura MEII universală. Cu toate acestea, conceptul este valabil ca o ghidare a conceptului arhitectural. Bazată pe interviuri extensive, studii detaliate ale arhitecturilor câtorva sisteme răspândite și importante și analiza de literatura privind vulnerabilitățile și riscurile în sisteme informaționale, a fost dezvoltată o metodologie de asistare pentru dezvoltarea caracteristicilor MEII în sistemele informaționale viitoare.

Metodologia constă din (1) identificarea funcțiilor informaționale ce sunt esențiale pentru misiunea unității; (2) determinarea sistemelor informaționale ce sunt esențiale pentru îndeplinirea acestor funcții; (3) căutarea vulnerabilităților în cadrul acestor componente de sisteme; (4) aplicarea tehnicilor de protecție adecvată pentru vulnerabilitățile găsite la diferite niveluri ale sistemului și (5) testarea protecțiilor împotriva unui set de scenarii de amenințare pentru a verifica robustețea lor. Aplicarea acestei metodologii va avea că rezultat o formă de MEII ce este un set de sisteme în structuri implicate de securitate sporită.

Scopul unei infrastructuri pentru asigurarea cercetării și dezvoltării (R&D) este de a susține dezvoltarea tehnologiilor care vor contoriza amenințările și vor reduce vulnerabilitățile în acele domenii ce au potențialul unui impact semnificativ asupra securității naționale, economiei și societății. Sunt avute în vedere amenințările fizice și informaționale. Tehnologiile considerate specifice sunt acelea care protejează infrastructura și astfel reduc vulnerabilitatea, detectează intruziunile și furnizează avertismente, tratează efectele de disfuncționalități (incidente), asigură asistență pentru managementul incidentelor și facilitează recuperarea.

Punctele focale ale programului sunt: (1) dezvoltarea tehnologiilor ce susțin recunoașterea rapidă a atacurilor la scară mare, (2) dezvoltarea sistemelor ce înglobează inerent caracteristici de supraviețuire, de exemplu capacitatea de a continua

operarea în situația atacurilor ce au succes parțial. Obiectivele specifice sunt: (a) recunoașterea atacurilor la scară națională și distingerea lor de evenimentele cu semnificație locală; (b) limitarea impactului unui atac prin asigurarea integrității datelor și programelor; și (c) împiedicarea atacurilor de interzicere a serviciului prin limitarea consumului de resurse ce poate fi făcut de un atacator. În final, trebuie să realizăm că multe dintre infrastructurile critice devin tot mai mult internaționale. Aceasta este o consecință logică a creșterii globalizării.

Între timp, câteva inițiative de protecție a infrastructurilor critice sunt în pregătire în Europa (ex. Uniunea Europeană, Germania, UK). Complementar cu inițiativele naționale în Europa, Comisia Europeana studiază stabilirea unei Inițiative de Dependabilitate Europeană ale Programului de Tehnologii Informaționale pentru Societate.

Această activitate este îndeplinită cu ajutorul Centrului de Cercetare Integrat, Institutului pentru Sisteme, Informatică și Siguranță. Studiile inițiate de Comisia Europeană introduc și explorează conceptul de supraviețuire. El evidențiază distincția între perspectiva de dependabilitate tradițională și punctul de vedere curent studiat în prezent în domeniul supraviețuirii.

Raportarea și analizarea incidentelor de securitate va rămâne pentru mult timp o problemă nerezolvată, dacă numai un atac din 20 este reținut de către victimă și numai un atac din 20 este raportat. Într-un studiu neobișnuit de larg și de stringent, Howard a analizat tendințele în domeniul securității Internet printr-o investigare a 4299 de incidente de securitate pe Internet raportate de Centrul de Coordonare CERT (CERT/CC) din 1989 până în 1995

Înainte de această cercetare, cunoștințele noastre despre problemele de securitate pe Internet au fost limitate și în principiu doar anecdote. Cercetarea desfășurată de Howard a îndeplinit următoarele: (1) dezvoltarea unei taxonomii pentru clasificarea atacurilor și incidentelor Internet, (2) organizarea, clasificarea și analiza înregistrarilor incidentelor raportate de CERT/CC și (3)

dezvoltarea recomandărilor pentru îmbunătățirea securității, Internet și pentru obținerea și distribuirea informațiilor despre securitatea Internet.

Cu excepția atacurilor de interzicere a serviciului, incidentele de securitate au fost găsite în general ca fiind în descreștere relativ la dimensiunea Internet. Estimările bazate pe această cercetare că un domeniu Internet obișnuit a fost implicat în medie la un incident pe an și un post Internet obișnuit a fost implicat într-un incident odată la 45 de ani.

Taxonomia atacurilor asupra calculatoarelor și rețelelor dezvoltată în această cercetare a fost utilizată pentru a prezenta un rezumat al frecventei relative al diferitelor metode de operare și a acțiunilor corective. Aceasta a fost urmată de o analiză a trei subgrupuri: (1) un studiu de caz a unui site care a raportat toate incidentele, (2) 22 de incidente care au fost identificate în înregistrări, prin diferite metode, ca fiind cele mai severe și (3) incidente de interzicere a serviciului.

Datele de la toate incidentele și de la aceste trei subgrupuri au fost folosite pentru a estima întreaga activitate de incidente Internet pe timpul perioadei de cercetare. Aceasta a fost urmată de o evaluare critică a utilității taxonomiei dezvoltate prin această cercetare.

Analiza concluzionează cu recomandări pentru utilizatorii Internet, furnizorii Internet, echipele de răspuns și guvernul SUA. Studiul lui Howard prezintă numai o analiză preliminară a datelor rezultate din înregistrările incidentelor în perioada 1989-1995. A fost recomandat că setul de date ar trebui făcut disponibil on-line pentru utilizarea de către alți cercetatori. Suplimentar, informații referitoare la analiza incidentelor, problemele metodice asociate și utilizarea taxonomiilor este oferită de Cohen.

Corelat cu creșterea incidentelor de securitate, a apărut criminalitatea în domeniul calculatoarelor și utilizarea greșită, depinzând fără îndoială de proliferarea tehnologiilor de calcul și creșterii Internet. Partea din stânga a figurii 5 evidențiază numărul de raportori ce au raportat diferite tipuri de atacuri sau de utilizare

greșită relativ la resursele lor de calcul și telecomunicații, ordonate de la cel mai preponderent la cel mai puțin preponderent.

Partea din dreapta a figurii 5 prezintă pierderile în mii de dolari pentru incidente de aceste tipuri cu pierderi cuantificabile. Figurile arată că deși au fost contorizați viruși de cel mai mare număr al companiilor, 73% din raportori spunând că au detectat incidentele de acest tip, ele nu au contabilizat pierderile cele mai mari, care au fost atribuite accesului neautorizat de către utilizatori din interior și furtului de informații proprietar.

Ultimele două amenințări raportate, ascultarea activă și pasivă, a fost contabilizată pentru pierderi mici. Raportorii au spus că sursele cele mai probabile ale atacurilor sunt angajații nemulțumiți (80%), hackerii independenți (72%), corporațiile din țară (48%), corporațiile străine (29%) și guvernele străine (21%).

Siguranța informațională include totalitatea măsurilor de securitate necesare pentru a furniza un nivel de protecție acceptabil pentru o infrastructură și pentru datele vehiculate de o infrastructură. Mai recent, aspectul de supraviețuire a fost recunoscut ca o componentă critică. Supraviețuirea sistemelor include caracteristici de: toleranță la defectări; robustețe, răspuns adaptiv; distribuție și variabilitate; recuperare și restaurare.

În acest capitol, accentul se pune pe măsuri de securitate tehnică, dar și măsurile de securitate fizică și de personal sunt esențiale pentru protecția complementară. Securitatea la nivel fizic include controale pentru accesul fizic la facilități, protecția de eșecul utilităților de sprijin, dezastre naturale și multe alte amenințări.

Un model de politică de securitate formal reprezintă partea centrală a conceptului de încredere. El definește matematic o bază de calcul de încredere (TCB) ca un model abstract.

Modelul include noțiunea de securitate a stării pentru TCB, subiecți (utilizatori ce accesează TCB), obiecte (seturi de date în TCB) și acțiuni pe care TCB le realizează. Modelul descrie aceste acțiuni fundamentale și starea tranzițiilor TCB. Modelul permite analiza și furnizează un mijloc de dovedire că orice implementare a arhitecturii TCB rămâne întotdeuna într-o stare stabilă.

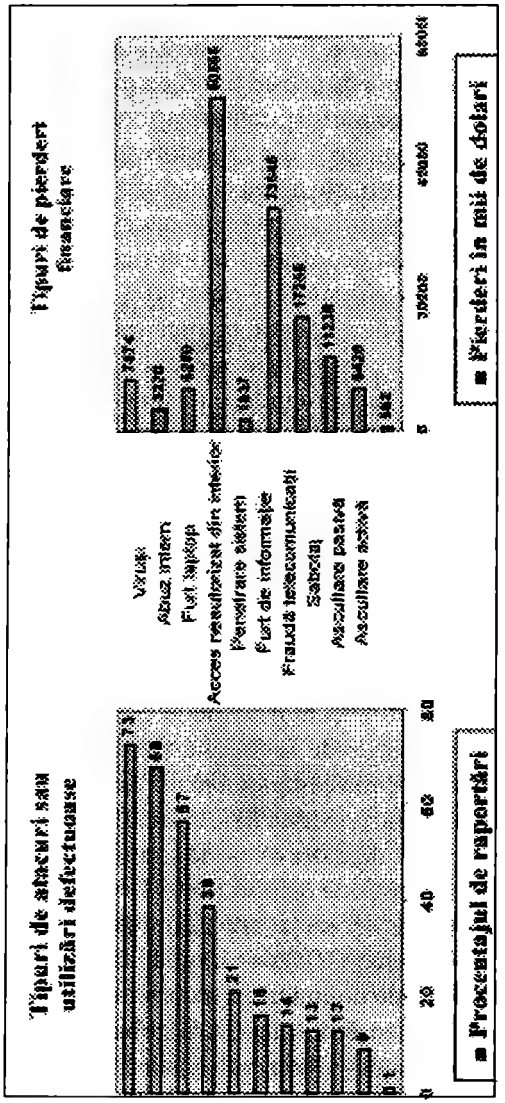


Figura 5: Criminalitate în domeniul calculatoarelor: Tipul de atac și pierderi financiare

Controlul accesului pentru autentificarea utilizatorilor reprezintă mecanismul de securitate fundamental a unui singur sistem sau a unor sisteme în rețea. Procesul de autentificare impune utilizatorului verificarea identității pentru a stabili accesul și restricțiile de control al accesului, procesele ce pot fi realizate de utilizatorul autentificat sau utilizatorii ce încearcă obținerea autentificării. Autentificarea unui utilizator într-o manieră sigură necesită un mecanism ce verifică identitatea utilizatorului la gradul de siguranță dorit.

Criptografia furnizează procesele matematice pentru transformarea datelor (prin criptare și decriptare) între un format deschis și un format de text cifrat pentru a furniza proprietăți private. Puterea algoritmului de criptare reprezintă o măsură a gradului în care textul cifrat suportă atacurile. Puterea finală și generalitatea prelucrărilor criptografice stă în formularea matematică a algoritmilor de transformare utilizați.

Sistemul de criptare general include calea la mesajul criptografic ce include procesul de criptare, transmisie și decriptare și o metodă suport pentru distribuirea unei variabile numerice, sau chei, care controlează transformarea de criptare. Generarea, stocarea, distribuirea și protecția de ansamblu a cheilor sunt critice pentru securitatea tuturor cripto-sistemelor. Cheile compromise furnizează mijloacele cele mai directe pentru accesul neautorizat. Din acest motiv, nivelurile de securitate fizic, informațional și perceptual trebuie să protejeze funcțiile de management a cheii, incluzând pe cele sintetizate mai jos. Suplimentar furnizării de intimitate, procesul de criptare furnizează un mijloc de autentificare a unui mesaj printr-un element de criptare a datelor numit semnătura digitală. Semnătura digitală permite dovedirea identității expeditorului și dovedește că atacatorul nu a modificat mesajul.

Zidurile de foc sunt sisteme de încredere care integrează autentificarea, controlul conexiunii, răspunsul la incidente, criptarea, securitatea structurii de rețea și conținutul de securitate

într-o singură unitate de securitate. Localizat între două rețele, tot traficul de trecere între rețele trebuie să treacă prin zidul de foc, care restricționează trecerea numai celor ce le este permis traficul prin politica de securitate.

Zidul de foc creează efectiv un „domeniu" de securitate sau o „enclavă", prin furnizarea unui perimetru de apărare pentru o rețea (domeniul securizat). Cele patru tipuri de bază ale zidurilor de foc sunt (1) filtre de pachete, (2) bazate pe circuite, (3) porți de aplicație și (4) filtre pachet dinamice.

Sistemele pentru detectarea intruziunii și răspunsului (IDS) sunt necesare pentru a proteja sistemele de calcul și rețelele de intruziuni interne sau externe. Securitatea calculatoarelor tradițională face distincția între activitatea de verificare și cea de raportare a alarmării.

Verificarea de securitate revizuiește înregistrările activităților pentru a detecta incidentele de securitate (incluzând schimbări în configurația operațională), pentru a verifica corespondența cu politica de securitate și a testa controalele de securitate. Raportarea alarmării de securitate monitorizează evenimentele legate de securitate care pot indica utilizarea greșită a controalelor sau configurațiilor de securitate, activități ostile împotriva controalelor de securitate sau comportamente inconsistente cu politica de securitate.

Detectarea automată a incidentelor, respectiv, raportarea și răspunsul de alarmare este necesar pentru a răspunde la atacuri de război informațional structurate asupra rețelelor. La fel ca în toate sistemele de alarmare, alarma falsă și ratele de detectare greșită măsoară în ansamblu performanța de detecție. Detecția automată și raportarea este necesară pentru un domeniu larg de acțiuni de amenințare, ex. intruziuni externe, intruziuni de securitate internă, eșecuri de sistem și comportare ciudată.

Cetățenii, industria, guvernul și militarii au devenit vulnerabili datorită bazării pe tehnologie, în particular tehnologii informaționale. Mai temător chiar, dar mai puțin înțeles, este că

această vulnerabilitate este sporită datorită bazării pe economia mondială și aranjamentelor de coaliție în domeniul militar. Deoarece imensitatea problemei siguranței informaționale (IA) în fața societății informaționale este neacoperită, o atenție sporită este acordată acestui subiect de către presă, industrie și guvern.

Domeniul siguranței informaționale se concentrează pe proiectarea sistemelor care poate să determine politici de securitate chiar în prezența codului daunător. Provocarea este de a proiecta, dezvolta și răspândi sisteme complexe cu încredere în posibilitatea lor de a satisface cerințe de securitate. Este în curs de dezvoltare o teorie a securității calculator care oferă o metodă formală pentru ingineria de securitate, așa încât ne putem aștepta să obținem tehnologii accesibile, verificabile, scalabile pentru o infrastructură a apărării robustă și sigură. Această teorie va avea trei componente: politica, mecanismul și siguranța.

Au fost făcute încercări pentru a aborda problema în creștere a siguranței informaționale. Unele dintre aceste încercări au fost tipic „reacționare", la nivel de suprafață, și cu concentrări înguste. De exemplu, zidurile de foc au fost introduse pentru a proteja rețelele de arie locală din Internet, oricum ele au fost dezvoltate la nivel superficial pentru a controla protocoalele și amenințările cunoscute care apăreau evidente. Mulți autori au arătat că există probleme inerente în procesele de proiectare și evaluare existente care creează sistemele noastre informaționale.

În concordanță cu DARPA, aceste probleme pot fi abordate numai printr-o schimbare fundamentală în filosofia de siguranță informațională. Este evident că metodele existente sunt inconsistente, ineficiente, nu abordează problemele dintr-un punct de vedere cu adevărat „la nivel sistem" și au scopuri și rezultate limitate de natură în prezent abstractă și imatură a disciplinei. Aceste limitări nu pot fi depășite cu cercetare de evoluție suplimentară în aceleași concepte cheie ca cele ale vulnerabilităților, amenințărilor și contramăsurilor.

În concordanță cu DARPA este necesară o nouă paradigmă de siguranță informațională - ceva ce face posibil pentru proiectant

și analist să culeagă și să probeze cauzalitatea, legăturile, și obiectivele întregului sistem. Un pas în știința de bază a siguranței informaționale ar trebui să fie dezvoltarea de echivalențe, legături, legi, logici, postulate, dovezi și metode de calcul așa încât metricile să poată fi utilizate efectiv.

La fel ca în alte discipline, complexitatea sistemelor nu va fi permisă pentru soluții închise, astfel va fi necesară modelarea siguranței informaționale. Scopul general al noii abordări DARPA este de a furniza un mediu științific pentru proiectare și evaluare care va duce la siguranță informațională îmbunătățită și va permite proiectarea și evaluarea mai rapidă la costuri mai mici. Acest mediu va consta din metode și mijloace automate ce furnizează rezultate și matrici consistente de evaluare a siguranței informațională.

Această muncă este realizată deoarece oamenii ce lucrează în prezent în domeniul proiectării și evaluării nu au nici o cale de a măsura consistent multe aspecte ale siguranței informaționale. Ei lucrează de asemenea fără un mediu integrat și un suport de unelte automate ce ar putea îmbunătăți pe scară largă performanța lor și siguranța sistemelor lor informaționale.

Unele analize ale metodelor și uneltelor necesare comunității de război informațional (IW) au avut ca rezultat un set important de descoperiri și recomandări. Evaluarea naturii problemei a condus la aprecierea că metodele de război informațional trebuie să fie în măsură să opereze cu procese complexe, dinamice, interactive și adaptabile, echipe de oameni sub stress, de culturi diferite și incertitudine ca o proprietate inerentă. S-a anticipat că va fi necesar un amestec divers de metode și tehnici pentru a ataca problemele din domeniile IW.

Aceste metode bazate pe unelte ar trebui să includă, dar nu să se limiteze la următoarele: (1) Expert în sinteză (ex. utilizarea mijloacelor structurate pentru judecăți de sinteză ale experților); (2) Modelare și Simulare Constructivă (ex. operatori simulați ce operează sisteme simulate); (3) Modelare și Simulare Virtuală

(ex. operatori reali ce operează sisteme simulate); (4) Modelare și Simulare Efectivă (ex. operatori reali ce operează sisteme reale).

Realizarea educării profesionale în domeniul războiului informațional (IW), siguranței informaționale (IA), și protecției infrastructurii critice (CIP) reprezintă o nevoie urgentă în toate organizațiile civile și militare ale tuturor țărilor deoarece cel mai important aspect al acestor trei domenii îl reprezintă oamenii. Pentru a face față acestor provocări trebuie să îmbunătățim atât calitatea cât și realizarea unei educații corespunzătoare.

Numărul personalului instruit special pentru securitatea sistemelor de calcul care pot să abordeze complexitatea tehnologiilor moderne și care sunt familiari cu abordările de securitate a sistemului este foarte redus.

Oamenii doresc securitatea, dar sunt confruntați cu două dificultăți. Mai întâi, ei nu știu cum să o obțină în contextul întreprinderii lor. Ei poate chiar nu cunosc o modalitate de a translata procedurile organizaționale în politici, cu atât mai puțin implementarea unui set de mecanisme pentru a forța aceste politici. În al doilea rând, ei nu au nici o modalitate de cunoaștere dacă mecanismele alese de ei sunt eficiente. Abordările educaționale moderne evidențiază siguranța informațională nu ca o simplă disciplină separată, ci ca o știință multi-disciplinară care include elemente ale sistemelor de operare, rețelelor, bazelor de date teoriei de calcul, limbajelor de programare, arhitecturii și interacțiunii om-calculator, încorporate ca apropiate în acest set de discipline.

În 1999 Organizația pentru Securitatea Sistemelor Informaționale a NSA (NSA/ISSO) a fondat un Program Național de Instruire și Educație INFOSEC (NIETP) cu șapte subprograme: (1) Șapte Centre de Excelență Academică în educația de siguranță informațională; (2) Colocviul Național pentru Educația de Securitate a Sistemelor de Calcul; (3) Programul Universitar Extins; (4) Programul Curriculum - A - de Dezvoltare Electronică; (5) Inițiativa „Cutia Albastră"; (6) Programul de Consultare Profesorală a Serviciului Academic; (7) Cursuri de Siguranță Informațională și de Evaluare a Proceselor.

Obiectivele Colocviului Național sunt de a crea un mediu pentru schimbul și dialogul între liderii din guvern, industrie și academii, referitor la nevoia și utilitatea educării în domeniul securității și siguranței informaționale. Dat fiind scopul și starea fluidă a cunoștintelor despre securitatea informațională, Colocviul va încerca să promoveze dezvoltarea preocupărilor academice care recunosc nevoia exprimată de guvern și industrie, și este bazată pe „cele mai bune practici" disponibile în domeniu. Colocviul va asista instituțiile educaționale pentru promovarea dezvoltării continue și partajarea resurselor educaționale de securitate informațională.

Cursul de război informațional (IW) al Școlii Postuniversitare Navale (NPS), Monterey, este proiectat pentru a furniza studenților posibilitatea de a aplica analiza și teoria inginerească de sistem, fundamentală pentru probleme sistem de IW întâlnite într-un mediu operațional. Studenții pot modela un sistem informațional generic, pot aplica teoria de proiectare inginerească a sistemelor și pot face prelucrări pentru a dezvolta un sistem de IW relevant.

Ei ar putea să învețe să aleagă abordări ce par inginerești pentru a apăra sistemul aflat în studiu și respectiv pentru a ataca sistemul dacă se presupune posesia lui de către un adversar. Cursul poate fi coordonat utilizând pas cu pas procesul de analiză a deciziei. De exemplu, analizele căilor nodale și critice pot fi revizuite pentru vulnerabilități, cu accent pe tendințele tehnologice în domeniile comunicațiilor și calculatoarelor.

Sistemele de decizie organizațională (comandă și control) și ingineria factorilor umani va fi studiată în scopul de a permite modelarea adversarilor militari și structurii de comandă civile ca parte a proiectului. Poate fi un proiect de curs (cu două echipe în competiție) destinat pentru formularea și prezentarea sistemelor unei organizații, pentru rezolvarea aplicațiilor operaționale specifice provocărilor de război informațional, utilizând echipamentul de comunicație selectat.

CONCLUZII

Cu douăzeci de ani în urmă, infrastructurile informaționale ale corporațiilor și cele militare erau separate și distincte și termenul de „război informațional" nu exista. Astăzi ele sunt pe cale să devină unul și același, și sistemele informaționale conectate în rețea rezultate, deschid multe uși pentru războiul informațional. Comunitatea militară depinde de aceleași (sau aproape aceleași) rețele de calcul și echipamente de rețea pentru a lupta în războaie cu cele de care depinde sectorul industrial pentru a conduce afacerile.

În acest scop, este important de subliniat că peste 95% din legăturile de comunicație ale SUA utilizează linii și sateliți comerciali, închiriați și pe timpul operațiunii Furtună în Deșert, procentul a fost chiar mai mare. Guvernul are trei roluri referitoare la infrastructura informațională națională: să fie gata să facă față amenințărilor iminente, să impună reguli adecvate, să promoveze confidența publică. Această lucrare ar putea să ajute la deschiderea unui dialog între academie, industrie și guvern, înspre asigurarea infrastructurilor informaționale și sistemelor informaționale.

Comunitatea de securitate are nevoie de un vocabular comun pentru a discuta amenințările și contramăsurile, și o metodologie comună de descoperire a vulnerabilităților din sistem, stabilirea unei priorități în termeni de pericole relative și determinarea costului efectiv al contramăsurilor.

Astfel, există un domeniu de probleme comune în contextul războiului informațional, cu provocări pentru un nou nivel de cooperare în știință, inginerie, și educație - dar multe dintre aceste probleme continuă să rămână nerezolvate pentru cooperare. Așa cum s-a prezentat în figura 1, domeniile războiului informațional (IW), securității informaționale (INFOSEC), și protecției infrastructurii critice (CIP) sunt împreună și ar trebui să lucrăm ținând cont de inter-legăturile dintre subdomeniile lor.

RĂZBOIUL CUNOAȘTERII

RICHARD SZAFRANSKI

Tezele dezvoltate aici se referă la cât de mult mai au de învățat militarii și autoritățile naționale despre integrarea efectivă a operațiilor informaționale în operațiile de securitate, pe timp de război sau de pace. La nivelul actual, la care se găsesc democrațiile vestice și cele nou admise în Uniunea Europeană, acestea pot ceda în fața acelor state, hackeri sau criminali care se adaptează mai repede la aceste instrumente. Acestea fiind spuse, nu intenționez ca acest material să devină echivalentul cărții „Al treilea val". Cu toate acestea, este un material care cheamă la acțiune.

Războiul informațional ofensiv, utilizează, pe scurt, tehnologiile informatice și alte capacități pentru a ataca infrastructurile bazate pe informații ale adversarului. „Comisia președintelui SUA privind protecția infrastructurii critice" este îngrijorată de echipamentele speciale cerute pentru a lansa atacuri RI asupra sistemelor de calculatoare americane. Instrumentele de atac de bază (calculatorul, modemul, telefonul NET-ul și programele software) sunt, în general, aceleași cu cele pe care le utilizează hackerii și criminalii. Comparându-le cu forțele militare și armele care amenințau în trecut infrastructurile americane, instrumentele RI sunt ieftine și rapid de obținut [84].

Mișcarea de la ceva vechi și familiar, spre ceva nou și necunoscut, este un proces dificil pentru oricine și mai ales pentru infanteriști, marinari și aviatori. După cum remarca Hart, nimic

[84] Comisia președintelui SUA privind protecția infrastructurii critice, p. 30.

nu e mai greu decât o înlocuire a vechilor idei. Atunci când infanteriștii, marinarii, și aviatorii cred că au ajuns să știe totul despre arta operațiilor, o nouă descoperire (de obicei tehnologică sau o aplicație) transformă elementele considerate până acum nesemnificative. Când se întamplă acest lucru, Zeul Marte se bucură. Trebuie să privim în trecut pentru a vedea viitorul.

Imaginați-vă cât de greu trebuie să le fi fost militarilor să accepte și să se acomodeze cu tehnologiile artificiale ale armelor de foc și ale tunurilor. A înjunghia, a răni, a zdrobi victima pare să mimeze vânătoarea perfectă, iar vânătoarea în haită sau pluton este o activitate care poate fi naturală speciei noastre. Noile competențe în chimie, metalurgie, inginerie, au trebuit să se dezvolte în tandem cu noi organizații și scheme de angajare. Armele de foc și tunurile au schimbat modul de a vâna al oamenilor. Armele de foc au constituit unul dintre elementele care au condus la transformarea corăbiilor, vapoarelor. Vapoarele cu aburi le-au înlocuit pe cele cu pânze, motoarele au înlocuit vaporii, doar pentru a vedea întoarcerea acestora sub forma puterii nucleare. Vapoarele au fost martorele creșterii influenței zonei subacvatice, în timp ce avioanele au devenit mesagerul câmpului de luptă aerian, ca principal mijloc de putere, de protecție.

Tehnologia aparaturii cu combustie internă și aplicațiile sale terestre au înlocuit caii și au condus la o reinterpretare a strategiei războiului. Și atunci au apărut mașinile zburatoare în nenumăratele lor variante. Armata încearcă permanent să se adapteze.

Însă atunci apar rachetele și armele nucleare, și spațiul cosmic Cercetările germane asupra vehiculelor destinate să poarte arme convenționale ne-au dat rachete balistice și de croazieră. Armele nucleare au dat acestor rachete energia necesară. Armele de precizie de lungă distanță, nucleare sau nu, care se autoghidează, permit forțelor armate să stea departe de câmpul de luptă și să provoace pierderi adversarului. Toate forțele armate doresc aceste arme convenționale sau nu și le folosesc într-un mod atât de mare încât ar șoca un om de rînd.

Armele de precizie care acționează la distanță reprezintă acum *lingua franca* a războiului. Forțele armate se ceartă, au opinii diferite în privința a ceea ce înseamnă acest lucru pentru război, pentru misiunile lor separate, pentru diferențierea operațiilor în mediile „lor" și pentru rolul forțelor aeriene și cosmice. Forțele terestre, aeriene și navale încearcă să ocolească aceste schimbări, și mărturie stau dezbaterile care precedă orice operație semnificativă. Însă armatele știu că noțiuni, ca „puterea de a zbura", depășesc puterea de acceptare a publicului versus „operații sângeroase". Voința de a se angaja formal în astfel de operații așează armatele mai aproape de putere. Chiar și armatele apreciază că riscul real la care se expune o țară în lumea de azi nu este invazia unei alte armate, ci puterea de a zbura și terorismul. Puterea de a zbura devine azi forța dominantă?

Nu. Adevăratul risc nu mai sunt armele de precizie și nici vehiculele zburătoare, ci noile descoperiri. Acestea, gravitând în jurul ideii de „noutăți intangibile" nu elimină vechile „mijloace" de luptă, însă le permit să se dezvolte sau, în unele cazuri, să fie înlocuite de noile descoperiri. Toffler a scris că: „Nimic nu sugerează că resursele și tehnologiile materiale vor dispărea. Evident, lucrurile contează, și mai ales armele. Software are încă nevoie de hardware. Soldații nu pot mânca date. Și legăturile fundamentale dintre instrumentele tangibile și ceea ce am putea numi „noile instrumente intangibile" sunt cruciale pentru eficiența militară, în ducerea războiului, cât și în încercarea de a-l preveni"[85].

Războiul informațional este noua mare descoperire pe care acoliții Zeului Marte trebuie s-o întâmpine. Marte, doar „ne-a dat" computerele, iar acestea „ne-au învățat" că tot ce ne înconjoară poate fi redus la o combinație de zero și unu. Această înțelegere a lansat epoca informațională, în care aceste combinații pot fi transmise electronic ca date și recombinate de cel care le primește, pentru a forma bazele unei informații. După părerea lui Arquilla

[85] A. și H. Tofiler, „Foreward: The New Intangibles", *In Athena's Camp: Preparing for the Conflict in the Information Age*, RAND, 1997

și Ronfeldt, „informația" reprezintă mai mult decât conținutul sau înțelesul unui mesaj, „informația este orice diferență care face diferența"[86]. Amenințarea faptului că aproape orice poate avea semnificație militară în lumea exterioară, a lansat epoca războiului informațional.

Războiul informațional este dificil să devină apanajul unor instituții, deoarece este o modalitate de acțiune indirectă și subtilă și nu una directă și brutală. Războiul informațional este o formă a conflictului, care atacă sistemele informaționale (carbonul și siliconul ca *mijloace* de atac al cunoștințelor sau crezurilor adversarului). Războiul informațional poate fi văzut că o componentă a unor activități ostile mai mari (ceea ce Arquilla și Ronfeldt numesc *netwar* sau *cyberwar)* sau poate fi înțeles ca unica formă a unei activități ostile. Războiul informațional se poate duce *în timpul* războiului sau *în afara* lui.

Să citim cu atenție ceea ce promovează US Force ca doctrină. Potrivit US Force, războiul informațional cuprinde acele „(...) operații informaționale care sunt executate pentru a-și apăra propriile informații și sisteme informaționale, afectând informația adversarului și sistemele sale informaționale. Aspectul defensiv este operațional în permanență. În schimb, aspectul ofensiv este, **în primul rând**, pus în aplicare pe timp de criză și de conflict. Războiul informațional include diverse activități ca operații psihologice, înșelare militară, război electronic, atacuri fizice și informaționale și o serie de activități și programe de apărare. Este important să se accentueze faptul că *războiul informațional* este o construcție care se execută de-a lungul întregului spectru, de la pace la război, pentru a permite aplicarea efectivă a responsabilităților Forțelor Aeriene"[87].

Războiul informațional cuprinde operațiile informaționale

[86] J. Arquilla și D. Ronfeldt, „Cyberwar is Coming!", *Comparative Strategy* 2, 1993.

[87] United States Air Force, „Information Operations", *Air Force Doctrine Document* 2-5, 05.08.1998.

duse pentru a apăra propriile informații și sisteme informaționale sau pentru a ataca și afecta informațiile și sistemele informaționale ale adversarului. Acest război e condus în primul rând pe timp de criză și conflict. Totuși, componenta defensivă, mai mult decât ofensiva aeriană, e condusă de-a lungul spectrului, de la pace la război"[88].

Războiul informațional ofensiv, „contra-informațiile ofensive" cum le numește USAF, sunt duse *în primul rând,* dar nu *exclusiv* „pe timp de criză sau conflict". Acest tip de război e *nou* și noutatea a fost întotdeauna o provocare.

Nu este nevoie de panică, ci doar de a lua lucrurile în serios. O motivație puternică pentru schimbare se cuvine să fie avertizarea privind perturbațiile serioase pe care le poate aduce războiul informațional doar prin încercarea de a modifica câmpul de luptă. Orice tulburare serioasă în sistemele informaționale poate reduce eficiența operațiilor. Să analizăm cunoscuta de acum problemă Y2K [89]. Așa cum spunea și senatorul Robert Bennett, vorbind despre această problemă, „antidotul panicii este informația curată, dar anumite informații curate pot fi infricoșatoare"[90].

La un nivel mai redus al agravării, grupuri mici sau state pot utiliza războiul informațional pentru a dezbina o mare parte a funcțiilor unui alt stat. La un nivel mai ridicat, grupurile mici sau statele pot afecta serios marile state [91]. Aceștia pot duce un „război informațional strategic" sau pot poseda capacități de „război informațional strategic". Capacitățile strategice sunt cele care pot da „lovituri serioase" securității altora sau securității intereselor altora.

---

[88] *Air Force Doctrine Document2-5.*

[89] Andrew Hay, „Top Y2K problem: Public Panic", Reuters, 22.06.1999.

[90] Jim Abrams, „Spreading the Y2K word without spreading panic", 08.06.1999, www.nandotimes.com

[91] A se vedea *The President's Commission on Critical Infrastructure Protection,* pag 30, oct. 1998.

Dacă contra-războiul informațional ofensiv poate fi dus în afara războiului, războiul informațional strategic poate fi și el realizat fără o declarație de război [92].

De aceea, trebuie să ne pregătim pentru astfel de acțiuni încă de acum, deși „Defensive Science Board" a estimat încă din noiembrie 1996 că avem ceva timp la dispoziție: „capacitățile de război informațional strategic" utilizate împotriva noastră se află încă la o distanță de șapte-zece ani depărtare [93]. Așa să fie?

Un studiu al RAND notează că: „O evaluare macro a stadiului primei generații a războiului informațional strategic al SUA și al altor state (sau a altor părți), în termeni de capacități absolute și relative de război informațional strategic ofensiv și defensiv ar fi dificil de realizat, chiar și la un nivel secret. Caracterul dinamic actual al revoluției informaționale și caracterul embrionar al războiului informațional strategic ca potențial instrument politico-militar, conduc la ideea unei abordări mai precaute în a face o astfel de evaluare, secretă sau nu, pentru prezent sau viitor" [94].

Fără a pune un mare accent pe „viitor", aproape toți sunt de acord că „în viitor există posibilitatea ca adversarii să exploateze instrumentele și tehnicile revoluției informaționale, pentru a ține piept riscului (nu pentru a distruge, ci pentru a dezbina pe scară largă sectoarele naționale strategice, cum ar fi diferite elemente ale infrastructurii naționale: energia, telecomunicațiile, transportul și finanțele" [95].

---

[92] Adam Herbert, „Air Force Official Calls Reduced Cycle Times Key To Info Superiority", Inside the Air Force, 21.06.1999. Potrivit articolului, Donahue (directorul comunicațiilor și informațiilor aviației militare americane) a numit forța aliată „epoca ciber-războiului" din cauza încercărilor sârbilor de a ataca sistemele informaționale americane. „Din fericire, acestea au fost la fel de eficiente ca și apărarea lor aeriană, a glumit el".

[93] Defensive Science Board, Task Force on Information Warfare-Defense, îl.1996. Duane Andrews, președinte, apreciază că o dereglare majoră strategică e de „joasă intensitate" până în 2005.

[94] Ibid.

[95] „Executive Summary", *Strategic Information Warfare Rising*, (MR-964.OSD9).

Ar fi un act de iresponsabilitate să se ignore riscurile unor astfel de atacuri, considerându-le ca fiind imposibile. Ar trebui să luăm în considerare amenințările și riscurile pentru a determina formele pregătirii și răspunsului nostru.

Analiștii de la RAND văd două amenințări la adresa SUA:

1. Amenințare la adresa securității economice naționale. Elementele infrastructurii naționale pot fi supuse unor dezbinări produse de un atac care are succes. Acestea pot avea efecte strategice, printre altele, pierderea încrederii populației în puterea de realizare a serviciilor infrastructurilor atacate.

2. Amenințare la adresa strategiei militare naționale. Există posibilitatea ca un adversar regional să utilizeze amenințări sau atacuri tipice războiului informațional strategic, pentru a deteriora sau a dezbina planurile americane dintr-o anumită zonă de criză.

Economiile sunt tot mai dependente de infrastructura informațională. Orice afectează deliberat, într-un mod răuvoitor, capacitățile acelei infrastructuri poate fi numit atac. Dacă există instrumente informaționale de distrugere sau de dezbinare care să afecteze tranzacțiile financiare, băncile, serviciile de investiții on-line, generatoarele de energie sau de distribuție, telefoanele sau centrele de distribuire a informațiilor, serviciile de urgență, etc., atunci, cel mai bun moment pentru un atacator de a face un test a fost perioada manifestărilor problemei Y2K.Problema Y2K este tratată aici ca un exemplu, ca posibilitate, chiar dacă ea pe moment s-a dovedit o alarmă falsă

Dacă SUA sau o alta țară sunt țintele unui viitor război informațional strategic, atunci este probabil ca statele mici sau municipalitățile unui stat să devină ținte ale testelor pentru atacurile de tip Y2K. Orașele din Europa de Est, din Orientul Mijlociu, din Asia de Sud, din America de Sud pot fi printre adversarii pe care trebuie să-i considerăm serioși. Analizele de ținte vor arăta entități particulare din cadrul statului candidat care sunt, în mod special,

vulnerabile (probabil o bancă sau o companie de telecomunicații)[96]. Cyber-atacurile ar prezenta un teribil avantaj: datele.

Un atacator va învăta multe despre modul în care statele răspund în fața unor inexplicabile probleme la nivelul infrastructurilor critice. Cum încearcă un stat să-și protejeze sistemele fizice sau virtuale esențiale pentru astfel de operații? Cum afectează atacurile asupra unor state mici economia interconectată? Ce puteri separate și ce legături există între forțele armate și autoritățile civile? Dar între guvern și actorii comerciali? Ce pare să meargă bine și ce nu? Ce sisteme sau elemente de infrastructură ne creează probleme mai mari? Cât de mult durează remedierea și care sunt impedimentele unei remedieri rapide? Încrederea populației este afectată?

Încă gândim proiectarea puterii în termeni de instrumente fizice și încă gândim interzicerea accesului ca instrument de negare a abilității de mișcare a masei. „Accesul" poate fi abilitatea de a se apropia de un loc fizic sau de a introduce un grup acolo, dar accesul fizic este doar *o formă* a accesului. Există „locuri" electronice. Există elemente de acces pe piață.

Există un acces la realitate și adevăr. În epoca informațională, instrumentele puterii se schimba [97]. Cunoașterea devine tot mai importantă, utilizarea ei conduce la acumularea bogăției și violența e transformată prin luarea unui avantaj asupra ei. În secolul următor „accesul interzis" va fi prezent sub multe forme: incapacitatea de a introduce marfa, incapacitatea de a o susține, incapacitatea de a participa pe o piață, și de a cunoaște adevărul. Însă unele din aceste fapte nu vor constitui un „acces interzis" prin ele însele.

Statele percep taxe pentru a împiedica un alt stat să-și vândă mai ieftin produsele pe piața sa. Războiul comercial este în plină

[96] Jube Shiver, „Phone Firms may have a few Y2K Hang-Ups", *Los Angeles Times*, 24.05.1999.

[97] Alvin și Heidi Toffler, *Powershift: Knowledge, Wealth and Violence at the Edge of the* 21 *Century*, Bantam Books, NY, 1990.

desfășurare. Ministerul indian al Comerțului a declarat că „lipsa capacităților comerțului în țara sa poate deveni o barieră a comerțului non-tarifar, împotriva exporturilor indiene într-o lume mai bună"[98]. Instrumentele non-violente pentru negarea accesului abundă deja și războiul informațional le va face pe toate mai subtile și mai elegante. Scopurile războiului informațional sunt cunoașterea sistemelor adversarului și exploatarea în propriul avantaj a slăbiciunii adversarului.

Imaginați-vă impactul interzicerii accesului unei piețe. Un anume întreprinzător încearcă să stăpânească o piață, să-și păstreze partea sau să capteze elementele critice, totul în scopul împiedicării accesului la această piață, sau ridicând costurile de intrare pentru noii competitori. În acest sens, multe companii aeriene de telefoane sau de alte utilități, au fost acuzate că pun în aplicare strategii de împiedicare a accesului și a competiției.

Nu ar trebui să fim surprinși că indivizi (sau state care îi sponsorizează), sindicate criminale, oameni de afaceri încearcă să împiedice accesul altora la propria afacere. Ceea ce surprinde este faptul că legea și posesia unei afaceri legale poate preveni accesul. Da, anumite state puternice cred că pot lupta, în felul lor, împotriva acestor lucruri. Însă repertoriul global a instrumentelor de împiedicare a accesului continuă să crească și multe au implicații în domeniul securității naționale.

Cea mai bună utilizare a strategiilor de împiedicare a accesului este împiedicarea accesului la adevăr [99]. „Negarea și decepția" văzute în această lumină sunt instrumente de împiedicare a accesului perfect, pentru că împiedică accesul la adevăr. Chiar dacă sunt utilizate pentru a proteja spațiul lor privat, indivizii, grupurile sau statele pot împiedica accesul la cunoaștere și să mascheze semnificația lucrurilor și acțiunilor observate. Acestea nu sunt în mod necesar acte de război.

[98] „Indian Government Concerned over Lack of E-Comerce Capabilities", *Telecomworld-Wire*, 10.05.1999.

[99] Alvin și Heidi Toffler, „Beyond Future Shock: Conspiracies, the Media and the War for the World's Mind", Los Angeles Times Syndicate, 15.06.1999.

Uitându-ne pe lista de mai jos, putem observa că puține din elementele prezentate nu au participat la crearea cursului natural al lucrurilor. E puțin probabil că o proiectare sau o desfășurare de sisteme ar putea avea loc efectiv, dacă s-ar confrunta cu aceste elemente în mod simultan.

- Manifeste;
- Distrugerea sau blocarea serviciului telefonic;
- Bruierea undelor radio sau a celularelor;
- Închiderea centrului de îngrijire a copiilor;
- Răspândirea știrii că Ebola sau E-coli se află în apă;
- Activarea bombelor logistice;
- Cauzarea unei bruieri a traficului prin dirijarea eronată a avioanelor sau altor vehicule publice;
- Bruierea recepției TV;
- Dezactivarea celularelor;

Încă o dată, o ocazie excelentă pentru a testa aceste efecte, a fost momentul creat de confuzia problemei Y2K. Nu sugerez că cineva face acest lucru, ci mai degrabă că cineva o va face.

Fără a trezi toți dragonii teoriilor războiului rece trebuie să acceptăm că posedăm doctrine de utilizare a instrumentelor ostile cu intenții ostile înainte ca formele familiare de ostilitate să erupă. Ostilitatea reprezintă utilizarea instrumentelor în scopul de a subjuga voința adversarului. Adversarul e subjugat atunci când pare a se purta ca agresor sau ca parte care se apără, în același mod în care noi intenționăm să-l facem să se poarte [100].

Și această modificare de comportament poate să-și aducă aportul înainte ca tradiționalele (vechile) concepte ale operațiilor de luptă să fie luate. Nu este vorba mai mult de „război", decât de „pace", pentru că războiul este doar o parte a provocării asigurării securității în secolul XXI. Alvin și Heidi Toffler sugerează că „o revoluție în modul de a duce războiul, cere o revoluție în modul de a face pacea". „Pacea" trebuie să includă măsuri de „anti-

[100] Richard Szafranski, „Toward a Theory of Neocortical Warfare: Pursuing the Acme of Skill", *Military Review*, 11.1994.

război" pentru că fața cealaltă a războiului este „pacea", așa cum cealaltă parte a războiului este „anti-războiul" [101].

Competența în timp de pace și anti-război îi vor diferenția pe cei care conduc provocările securității în prima parte a secolului XXI. Toffler observa faptul potrivit căruia „cunoștințele reprezintă ceea ce anti-războiul va fi mâine". De aceea, e nevoie să se „accelereze colectarea, organizarea și gestionarea noilor cunoștințe, canalizându-le spre calea căutării păcii [102].

Un element important al noii cunoașteri de care avem nevoie este cunoașterea modului în care se utilizează războiul informațional, sau contra-informațiile ofensive, pentru a înăbuși voința ostilă. În acest scop, aș vrea să prezint câteva principii care ar trebui să ghideze democrațiile în căutarea și utilizarea acestor noi cunoștințe. Unele principii pot provoca dezbateri aprinse, totuși, țelul meu este să generez o nouă cunoaștere în căutarea capacităților efective de anti-război, pentru a prezerva pacea.

Aceste principii se referă la secret, modelare, integrare, la modul de a cădea de acord în declanșarea evenimentelor, la prevenire și la escaladare.

Așa cum este dificil într-o democrație să dezvolți în secret noi arme și capacități, orice cercetare și experimentare a capacităților de contra-informații ofensive, trebuie să beneficieze de măsuri de restricție drastice și să fie bine compartimentate. Anumite capacități naționale se cuvine să nu fie partajate cu aliații din cel puțin patru motive.

În primul rând, alianțele din următoarele decenii pot fi vremelnice și deci, instabile. Un aliat, la un anumit moment se poate afla de cealaltă parte. Capacitatea de a surprinde poate dispărea dacă unul dintre foștii amici cunoaște capacitățile acestuia. În al doilea rând, noile cunoștințe de orice fel sunt proprietăți intelectuale care pot fi evaluate.

---

[101] Alvin și Heidi Toffler, *War and Anti-War*.
[102] Alvin și Heidi Toffler, *War and Anti-War*, p. 241.

A plăti nota pentru dezvoltarea unei noi proprietăți intelectuale și apoi a capitula nu este, în mod tradițional, o afacere bună sau cel puțin, nu este o afacere bună de securitate națională. De exemplu, să dezvolți un nou cifru sau un nou cod pentru a proteja informația sau să dezvolți noi capacități de spargere a codurilor pentru ca apoi să renunți. În al treilea rând, există o legătură între orice nouă capacitate informațională și avantajele economice pe care aceasta le poate asigura posesorilor săi. De aceea, armele informaționale, față de armele atomice, pot avea componente de mare utilitate pentru a realiza produse și activități care nu au legătură cu sfera războiului. În al patrulea rând, nu ar fi inteligent să presupunem că celelalte state sau grupuri nu-și dezvoltă în secret, capacități de razboi al cunoașterii.

Pe de altă parte, a partaja anumite vulnerabilități și tehnici de exploatare ofensive poate avea o considerabilă recompensă atât pe termen scurt cât și pe termen lung. În primul rând, ar fi naiv să credem că cei care sunt angrenați în acest joc nu vor coopera pentru a acoperi largul spectru de atacuri care pot fi ușor dezvoltate de jucători de talie mult mai mică, dar dispersați în spațiu.

O protecție individuală a marilor jucători ar cere o multiplicare a eforturilor și o dezvoltare a marilor resurse (dar totuși finite) pentru a sprijini și a conferi forța unor mari organizații până la unele mai mici, mult mai concentrate asupra apărării și agresiunilor din sfera ciberspațiului.

În al doilea rând, introducerea amenințărilor adesea mărește stabilitatea și securitatea, prin stimularea dezvoltării și desfășurării măsurilor de protecție, a celor motivați să-și protejeze propriile sisteme. Cineva ar numi această tactică un „prezumtiv auto-atac"[103].

Nu în ultimul rând, și poate cel mai important, cel mai bun argument pentru partajarea cunoștințelor ar fi că un astfel de lucru

[103] Richard Szafranski, « Awareness, Adritness, Audacy », o introducere la « Mastery of Information: Technology and Operational Concepts Circa 2030 » simpozionul *Joint Experimentation Futures Workshop,* 04.05.1998

ar fi amplificat de efectele rețelei, un fenomen care a ajutat la crearea „exploziei cunoașterii", conduse de tehnologiile de comunicație. Deși un asemenea schimb ar cere părților o siguranță în privința obiectivelor comune pe termen lung, cea mai bună strategie ar fi să se echilibreze avantajul secretului cu beneficiile unor schimburi de cunoștințe [104].

Unii ar putea argumenta că o atitudine secretoasă poate conduce la o spargere a alianțelor sau la atacuri informaționale duse la întâmplare. Le voi răspunde că poate lumea deja este așa. Competiția la nivelul calculatoarelor, al aplicațiilor software și al telecomunicațiilor crește deja într-un ritm alert de cele două părți ale Atlanticului. Fiecare companie sau națiune speră să fie cu un pas înaintea celorlalte, pentru bogăția propriilor acționari. Ne aflăm deja aici.

Admit faptul că armele informaționale sunt o nouă categorie de arme, dar cu greu fac distincția între softul de anti-virus din zilele noastre și armura folosită pe vremuri. Pentru a realiza o activitate de contra-informație defensivă trebuie bine cunoscute capacitățile cerute pentru o activitate eficientă de contra-informație ofensivă.

Alianțele dintre state sunt puțin diferite de parteneriatele din afaceri. Statele au întotdeauna dreptul și obligația de a abroga chiar și cele mai solemne tratate în interes național. Încheierea unui parteneriat în afaceri păstrează aceleași prerogative. Ar fi naiv să se creadă că alianțele sunt construite pe altceva decât interesele fiecărui stat membru.

Statele mai mici decât SUA vor protesta, bineînțeles, împotriva realizării în secret și a nepartajării capacităților naționale americane (inclusiv ale războiului informațional) ca fiind o nouă manifestare de, imperialism sau de izolaționism. Însă SUA trebuie să se obișnuiască cu astfel de plângeri.

Secretul ne va expune pe toți la o creștere întâmplătoare și la

[104] Brian Witten a numit acest lucru « Efectul de rețea al cunoștințelor ».

o destabilizare a atacurilor informaționale? Ar trebui să-i întrebam pe hackeri și crackeri despre acest lucru. Instrumentele antidot dezvoltate în secret de state ar putea de fapt să mărească stabilitatea și să evite atacurile întâmplătoare. Un hacker care simte greutatea puterii unui stat sau capacitățile contrainformațiilor ofensive s-ar gândi de două ori înainte de a acționa.

Netul și Web-ul sunt noțiuni comune și orice stat ar trebui să se simtă liber să acționeze împotriva celor care nu au, o purtare corespunzătoare. Statele se vor comporta moderat, cred, cel puțin pentru că există o lipsă de tragere de inimă în a expune public existența armelor informaționale din arsenalul lor. Păstrarea secretului este baza accelerării colectării, organizării și generării acestor noi cunoștințe. Și păstrarea secretului este cheia pentru canalizarea acestor noi cunoștințe spre căutarea mijloacelor de anti-război. Dar păstrarea secretului nu e o măsură suficientă.

MODELAREA va fi un pas esențial în acest proces - dezvoltarea unei metode de abordare științifică pentru provocarea asigurării informaționale. Comportamentul componentelor și al sistemelor trebuie modelat (sistemele de stocare, comportamentul uman, erorile de sistem). Toate aceste modele trebuie să poată lucra împreună pentru a modela întregul sistem informațional și a cuantifica interdependențele modelelor separate. Modelul dezvoltat trebuie să țină seama de lucrările din trecut și să dezvolte cercetarea, inclusiv modelarea dinamică și sistemele bazate pe agenți [105].

Astăzi înțelegem mai puțin decât avem nevoie să înțelegem să ne apărăm împotriva atacurilor și să facem funcțional războiul informațional și ciber-războiul, pentru a aduce contribuții semnificative războiului, anti-războiului și păcii.

INTEGRAREA O dată ce putem modela operațiile informaționale trebuie să găsim căile eficiente de a integra

[105] Michael Skroch, «Development of a Science-Based Approach for Information Assurance». Defense Advanced Research Projects Agency, Information Systems Office, 10.05.1999.

capacitățile de război informațional în diplomație, anti-război și război. Cineva observa odată că diplomația este arta de a spune „frumos cățeluș, în timp ce ne uităm după un baston puternic".

Informația este cheia cunoașterii cățelului care mârâie, a motivului mârâitului, a ceea ce îl sperie, a dimensiunii pe care o poate lua bastonul și când și unde poate fi „aplicat". A aplica bastonul care trebuie cățelului este un lucru dificil, dar pentru a face acest lucru „cineva" trebuie să fie responsabil pentru integrare.

Poate cea mai bună integrare se face integrând substraturile diferitelor capacități. De exemplu, responsabilitatea privind mass-media trebuie acordată unui grup, iar comanda și controlul rețelelor de calculatoare unui alt grup. Integrarea închide orice legătură existentă între forțele terestre, spațiale și aeriene, la fel de bine ca și cele existente între afacerile externe, apărare, comerț, etc.

La urma urmei, integrarea și autoritatea trebuie să se găsească la șeful statului și la comandantul tuturor categoriilor de forțe armate. Cu cât sunt mai repede înțelese capacitățile războiului informațional ale unui stat, cu atât mai repede e nevoie de control și execuție centralizată. Probabil, paradigma controlului centralizat și al execuției descentralizate se va transforma într-o autoritate centralizată a execuției și a controlului descentralizat al instrumentelor.

Există astăzi asemenea agenții de integrare? Nu știm precis. Disputele recente nu au adus probe evidențe ale eficienței sau ineficienței aplicațiilor războiului informațional. Genocidul pare să fi fost tolerat în Rwanda și Iugoslavia, cu excepția loviturilor împotriva trupelor sârbești și a capacităților de control ale forțelor paramilitare UCK albaneze. De asemenea, constatăm că embargoul informațional rămâne fizic și electronic și impermeabil.

Scopul capacităților de integrare a operațiilor informaționale este de a face posibil anti-războiul. Anti-războiul, se opune activ izbucnirii războiului și necesită o mare atenție acordată evenimentelor trecute care au erupt în violență până la urmă. Integrarea operațiilor informaționale și capacitatea de a conduce operații

secrete, vor permite guvernelor să acționeze repede și fără a fi observate la cea mai mică comportare anormală. Un lucru nu trebuie să fie secret: categoriile comportării necorespunzătoare care cer un răspuns adecvat.

A CĂDEA DE ACORD ÎN DECLANȘAREA EVENIMENTELOR

Al doilea război mondial a fost un parametru al conduitei inadecvate, astăzi statele sunt mai permisive în privința unei proaste comportări a unui stat. Statul X își poate construi economia de export pe creșterea opiumului sau folosind abuziv copiii. Statul Y poate fi cel mai mare exportator de marijuana. Statul Z poate închide toți practicanții unui anumit grup etnic sau religios. Iar statul T poate reține toți teroriștii ceruți de statele X, Y, Z. Respectul nostru pentru lege dus la extrem ne obligă să negociem cu teroriștii, criminalii de război, până când procesul se consumă.

Se poate observa că standardele noastre de moralitate și legalitate nu pot fi făcute universale prin războaie violente, duse în afara limitelor noastre teritoriale. Totuși, nu pot crede că războiul informațional nu poate constitui un bun antidot pentru anumite forme ale unui comportament inadecvat, care nu se poate ridica ușor la nivelul declarației de „război".

Cu alte cuvinte, există evenimente a căror declanșare statele o pot recunoaște ca indezirabilă sau în condiții rele. Acestea pot fi ușor recunoscute în articolele care susțin motivația existenței ONU. La fel ca embargourile, operațiile informaționale pot asigura instrumente eficiente la constrângerile non-letale. Aparent ne lipsește capacitatea și curajul de a utiliza operațiile informaționale în situațiile în care comportarea rău-voitoare necesită a fi pedepsită.

Păstrarea secretului va permite dezvoltarea capacităților, iar integrarea va da capacitate, însă curajul este o chestiune a fiecărei evaluări de risc și a consecințelor asupra fiecărui stat. Statele puternice sunt mai tolerante la riscuri decât cele slabe. De ce statele

puternice nu s-ar pregăti să dea prioritate operațiilor informaționale?

PREVENIREA Aceasta este un instrument care cere contact fizic cu subiectul. David Ronfeldt, un strălucit cercetator de la RAND sugerează că democrațiile de tip „NET" se vor confrunta pe viitor cu „un nou model de conflict de joasă-intensitate, dar de un mare nivel social", foarte atrăgător pentru un lider care are trăsături psihologice nesănătoase [106] și „ale cărui țeluri vor fi de a opera încet și acoperit pentru a-și slabi adversarii". Identificarea din timp a unor asemenea caractere ar fi folositor.

În timp ce angajamentele fizice atrag atenția și presupun riscul pierderilor de vieți omenești, anumite operații de război informațional nu comportă aceleași riscuri. De aceea, ne putem aștepta ca acele capacități de război informațional create în secret și integrate atacurilor non-militare și non-tradiționale, ca și capacitățile de luptă tradiționale să fie utilizate la fel de repede pe cât se declanșează evenimentele.

Forțele de atac nu vor cere permisiunea nimănui, cu excepția șefului de stat, prietenii și aliații nu vor fi avertizați, și responsabilitatea nu va fi acceptată. Acest lucru va necesita o abordare a relației civili-militari diferită. O astfel de necesitate va schimba relațiile dintre luptători și cei care nu luptă, dintre autoritatea civilă și cea militară, și, bineînțeles, vom numi în continuare statele noastre „democrații".

Pentru aceste motive, dar și pentru multe altele, așteptăm noi concepte de operații informaționale. În viitor, statele ar putea cere utilizatorilor de Internet să-și imunizeze sistemele împotriva virușilor distrugători. Pentru a asigura atât bunăvoința cât și disponibilitatea, guvernul ar putea periodic să elibereze viruși în sistemele sale, la partenerii săi și inevitabil la noi.

---

[106] David Ronfeldt, „Beware the Hubris-Nemesis Complex: A Concept for Leadership Analysis", *RAND*, 1994.

Prevenirea ar putea deveni astfel o normă. Nu există încă o armă creată, pe care umanitatea să nu o fi folosit. Trebuie să credem că nu există nici o nouă armă, fapt care să reiasă din doctrina militară existentă în prezent și din aceste discuții despre războiul informațional?

ESCALADAREA Toffler se întreba „dacă un adversar utilizează instrumente intangibile pentru a distruge sau provoca pagube unei anumite rețele de calculatoare ale unui oraș, inclusiv ale poliției, ale autorităților aeroportuare, a sistemelor electrice, bancare, etc.. Chiar dacă se presupune că se identifică sursa atacului, situația cere o intervenție militară? A cui va fi responsabilitatea de a răspunde și cum se va face acest lucru? Și ce s-ar întâmpla dacă dezordinea provocată în oraș ar fi televizată în Mexic arătându-se imagini false despre măsurile brutale luate de poliție împotriva sud-americanilor din L.A.? Dacă ar exista un război informațional dus din interiorul și din exteriorul SUA, măsurile de răspuns ar fi responsabilitatea FBI sau a militarilor? [107].

Nu există răspunsuri simple la aceste întrebări. Știm că războiul informațional urmărește modelarea comportamentului uman, în funcție de scopurile sale. Ne putem închipui că panoplia armelor următoarei generații de război informațional va include instrumente create pentru a afecta creierul uman: sunete, mirosuri, gusturi, imagini, senzații tactile. Ar putea include chiar și droguri sau feromoni.

În acest caz, care nivel al atacului este just și proporționat și care este neașteptat, disproporționat sau injust? Există vreun nivel al răspunsului just și proporționat fără a cunoaște bine statul sau grupul atacat?

Armele informaționale sunt noi, șterg distincția dintre luptători și cei care nu luptă. Putem să ne punem aceleași întrebări ca în cazul forțelor nucleare? Ar împiedica statele războiul informațional? Cum? În același mod prin care cursa înarmării nucleare a fost stopată: prin atingerea unei capacități suficiente

[107] Alvin Toffler, „Foreward", *In Athena ' s Camp*, p.18.

pentru a nimici milioane de oameni? Sau ar trebui să creăm propriile noastre forțe informaționale pentru răspunsuri flexibile sau selective? Ar fi înțelept să avem anumite opțiuni de răspunsuri „limitate" de război informațional, dar să ținem în rezervă altele „nelimitate"? Ar opta statele pentru o „asigurare de distrugere informațională mutuală"? Am fi pregătiți să tergiversăm un război informațional?

Noțiunea probabilității erorii circulare va deveni instrumentul de calculat al probabilității erorii prin statisticile tehnice ale lanțului Markhov în războiul informațional?

Care sunt canoanele pagubelor epistemologice acceptate sau a probabilității pagubelor? Ce este o „pagubă informațională colaterală" și cum va fi controlată? Există o apărare civilă împotriva nivelului strategic de război informațional?

Cine va asigura managementul războiului informațional și cum? Va susține cineva „înghețarea armelor informaționale" sau o „zonă liberă" a acestora? Există multe alte întrebări referitoare la implicațiile războiului informațional.

Dacă războiul informațional nu este un lucru serios, cum se explică existența în SUA a unor entități ca „Centrul armatei privind activitățile de război informațional", „Centrul de război informațional al forțelor aeriene", „Activitatea navală submarină de război informațional", „Centrul flotei de război informațional"?

CONCLUZII

Războiul informațional reprezintă utilizarea cunoștințelor pentru a contopi cunoașterea cu acțiunea efectivă. Tehnologia se află deja aici, însă tehnicile așteaptă încă teste și procese. Cred că vom asista la o serie de teste și procese de tipul manifestărilor problemei Y2K.. Pentru a ne proteja și a proteja sistemele informaționale trebuie să facem mari progrese în modelarea, integrarea, securitatea acordului în declanșarea evenimentelor, înțelegerea prevenirii și a escalădării. Multe din acestea trebuie să se desfășoare în secret. Ceea ce va fi vizibil va fi nivelul reușitei noastre. Cunoașterea, după cum spunea Toffler, este lucrul despre care va fi vorba în războaiele și anti- războaiele de mâine.

REVOLUȚIA INFORMAȚIONALĂ

PATRICK TYRRELL*

Acest material examinează natura informației și observă cum aceasta se transformă, în epoca „post revoluției informaționale". A schimbat acest lucru modul în care o foloseam? A modificat maniera în care noi, ca oameni, răspundem la ea?

Voi încerca sa examinez, câteva potențiale amenințări și modul în care integritatea informației poate fi mai bine păstrată. Voi ridica o serie de probleme importante, dar la care nu există încă răspunsuri: cui revine responsabilitatea pentru păstrarea informației?

Cum poate un stat să-și exerseze suveranitatea asupra informației și fluxului informațional? Cum pot fi controlate rețelele globale și ce amenințări la adresa integrității informației naționale pot fi identificate? Acestea sunt câteva probleme care așteapta încă răspuns, lucru care nu ne va impiedica să ne aventurăm pe tărâmul informației.

„De abia acum începem să realizăm dimensiunea și profunzimea schimbărilor în condițiile vieții umane, proces care continuă să se desfășoare. Noțiunea de distanță se modifică, puterea fizică disponibilă a devenit foarte mare, suveranitatea statelor imposibilă".

H.G. Wells [108]

---

* Agenția serviciilor de apărare a comunicațiilor

[108] H,G.Wells, *A Short History of the World,* London Penguin, 1936.

„Electronul, după părerea mea, este precizia din urmă care ghidează muniția".

John Deutch
Director CIA [109]

Pe măsură ce ne apropiem de sfârșitul secolului XX, jurnaliști, scriitori, oameni de știință și comentatori s-au întrecut în a atinge un anumit grad de imortalitate cu ajutorul „biților de sunet". Un concept care s-a impus de la sine în conștiința publică este „revoluția informațională", având des o vagă înțelegere a ideilor implicate.

Un cuvânt care a pătruns în lexicul popular, ca rezultat al acestei revoluții este „ciberspațiul", inventat de un scriitor de science-fiction american în anii 80, observând câțiva băieți jucând jocuri pe calculator, foarte captivați de lumea virtuală.

Există un întreg comerț cu cărți, articole, reportaje sau discuții asupra implicațiilor revoluției informaționale în fiecare aspect al efortului uman. Nu putem concepe viața modernă fără convenienta, rapiditatea și universalitatea sistemelor informaționale de azi, de la modestul telefon la posibilitatea de a participa la discuții în grup pe Internet, de la cartea de credit la manipularea piețelor financiare, 24 de ore din 24.

Aceste exemple, ca multe altele, conduc la ideea că fluxul informațional nu poate fi împiedicat, că informația recepționată e corectă, și nu coruptă, și e cât se poate de clară. În multe cazuri, se va porni de la ideea că fluxul informațional e privat și că informația e confidențială între emițător și receptor.

Integritatea informației a fost întotdeauna o problemă de interese critice, însă schimbările dramatice introduse de revoluția informațională au făcut mult mai dificil de urmărit traseul pe care îl urmează informația de la un punct la altul.

---

[109] John Deutch, „Oral evidence to US Senate Committee of Government Affairs", The *Times*, 26.06.1996.

Tocmai această inabilitate de a identifica cu ușurință proveniența informației, la care se adaugă sistemele moderne care permit o interconectare globală, au permis dezvoltarea globală a crimei organizate, caracterizată ca fiind cea mai mare afacere, cu profituri estimate, în 1998, la un miliard de dolari. În domeniul militar, aceleași condiții au dat naștere conceptului de *război informațional,* prin care un potențial adversar poate încerca să exploateze vulnerabilitățile din cadrul sistemelor informaționale naționale ale unui stat.

Aș dori să examinez termenii care sunt des folosiți pentru a descrie anumite concepte care modelează perspectiva modernă a informației. Alvin și Heidi Toffler [110] includ în largul concept al cunoașterii informațiile, datele și cultura. Schwartau [111] consideră datele ca fapte individuale sau statistice într-o formă necorelată, care, odată organizate, devin informații.

Transformarea informației în cunoștințe se realizează în momentul în care intervin intuiția și gândirea umană. Un academician francez, Philippe Baumards [112] merge mai departe și argumentează că o societate fundamentată pe filosofia greco-romană, limitează bazele sale de cunoștințe mai degrabă la *„cunoștințe obiective"*, decât la cele incluzând perspective mai largi, cum ar fi *„cunoștințele conjuncturale"*. Baumard face astfel o distincție între *„informare"* și *„cunoaștere"*.

Acesta consideră că multe organizații, mai ales cele care funcționează în perioade de schimbări considerabile, cred că trebuie să utilizeze din ce în ce mai multe cunoștințe și acest lucru le forțează să proceseze tot mai multe informații. În opinia lui Baumard, organizațiile și indivizii care au succes acordă mai multă atenție „simțului practic", decât colectării simple de informații.

---

[110] Alvin și Heidi Toffler, *War and Anti-War - Survival at the Dawn of the 2rt Century,* Little, Brown&Co., 1993.

[111] Winn Schwartau, *information warfare - Chaos on the Electronic Superhighway,* Thunder's Mouth Press, New Zork, 1994.

[112] Ph. Baumard, *From InfoWar to Knowledge Warfare: Preparing for the Paradigm Shift,* InfoWar Con, Bruxelles, 05.1996.

Fukuyama [113] examinează rolul erei informaționale în erodarea ierarhiei și autorității în societate și accentuează rolul încrederii și partajării normelor etice, care reprezintă fundamentul unei societăți. O bună informație va spori abilitatea omenească de a raționa.

Valoarea *„informării"* este similară filosofiei lui Sun Tzu care spunea că un lucru important este să distrugi strategia adversarului înainte ca acesta s-o pună în practică. Acest lucru trebuie făcut într-o manieră neașteptată, printr-o utilizare neconvențională a „forței divine" *(ch'i)*.

Opusul lui *ch'i* este forța comună *(cheng)*. Pe câmpul de lupta, *cheng* e o forță care doboară adversarul imediat, în timp ce *ch'i* reprezintă manevra de flancare care distruge în mod fatal strategia inamică [114]. Acestea sunt și ideile care stau în spatele conceptului lui Edward de Bono *„gândirea paralelă"*: „În gândirea paralelă se pune un mare accent pe concepte și pe informație" [115].

De ce am fi interesați de aceste diferențe și cum ar putea ele să ne ajute să înțelegem problemele legate de integritatea informațională? Există o tendință aparent naturală, în domeniul tehnologiei informaționale, ca și în cel al tehnologiei în general, care permite tehnologiei să conducă dezvoltarea sistemelor care privesc mai ales, necesitățile societății sau pe cele ale organizațiilor. Înțelegerea aspectelor umane ale procesului decizional este importantă dacă dorim să ne oprim asupra zonelor în care integritatea poate fi vitală și să identificăm domeniile în care o siguranță a integrității e, cel puțin, la fel de importantă.

Doctrina militară de comandă-control (C2W) se axează pe ceea ce e nevoie pentru a influența comportamentul uman și definițiile includ utilizarea integrată a distrugerii fizice, a războiului electronic, a înșelătoriei, a operațiilor psihologice și a operațiilor de securitate.

---

[113] Francis Fukuyama, TRUST: The Social Virtues and the Creation of *Prosperity*, London, Hamish Hamilton, 1995.

[114] „Survey of Defense Tehnology", *The Economist*, 10.06.1995.

[115] Edward de Bono, *Parallel Thinking – From Socratic to de Bono Thinking*, Viking,1994.

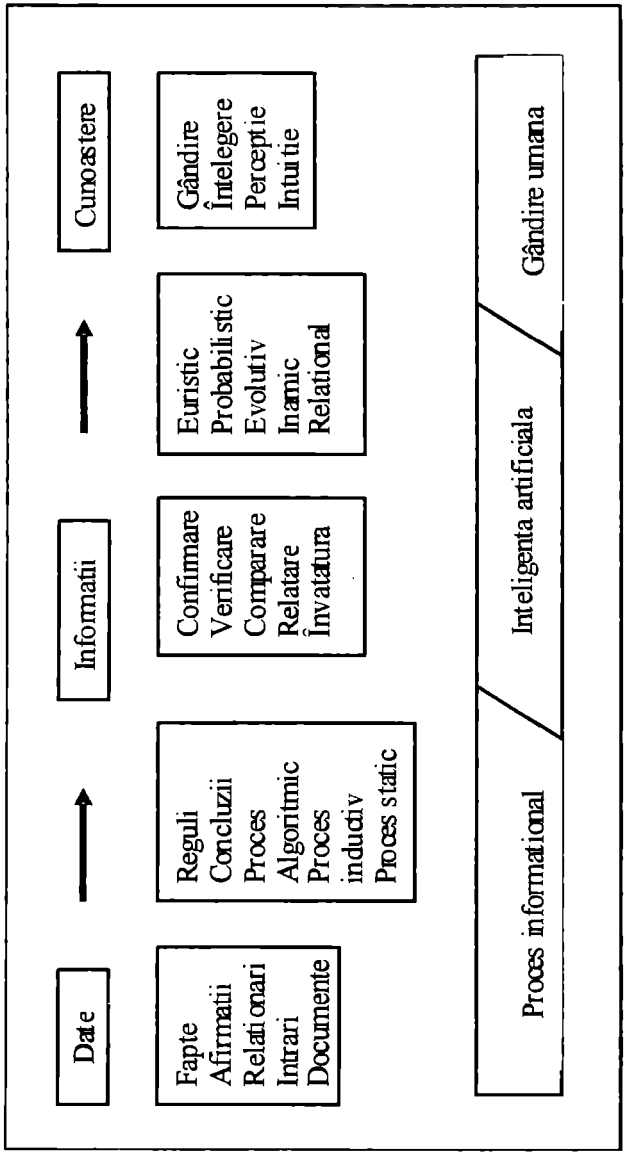


Figura 1: Spectrul cunoașterii

Utilizarea unor astfel de tehnici poate afecta modul în care un decident va interpreta informația, structurându-se după tendința sa naturală de a gândi mai mult inductiv decât „lateral". O astfel de viclenie de război posedă o bogată istorie, de la Calul troian la „Mary how never Was".

Este interesant de urmărit munca pe care au depus-o experții în sisteme [116], în care un atribut esențial al acestor sisteme comparate cu programele convenționale este natura euristică.

Este vorba de o revoluție a cunoașterii care scoate în evidență accentul pus pe fluxul informațional și accesibilitatea cunoștințelor. Conceptul „capital intelectual" e din ce în ce mai acceptat ca noțiune în lumea comerțului, ca unul din cele mai importante bunuri ale unei companii.

Dezvoltarea unui astfel de bun este cheia succesului, după cum o poate certifica creșterea fenomenală a anumitor companii Internet, ca *Amazon. com.* Este interesant să privim *Spectrul cunoașterii* din Fig. 1. Acesta ilustrează legăturile dintre un anumit număr de concepte și procesele de control ale transformării datelor în informații, de virtuțile umane tradiționale prin care informația devine cunoaștere.

Există și patru stadii cheie ale ciclului de viață al informației: crearea, culegerea, diseminarea și utilizarea ei.

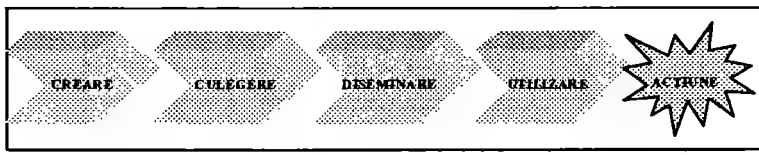


Figura 2: Ciclul de viață al informației

Aceste patru cicluri sunt distincte, deși au multe caracteristici în comun. Dezvoltarea tehnologică din ultimii ani a afectat viteza și volumul culegerii și diseminării informației. Pentru a fi eficaci,

[116] Peppard, IT Strategy for Bussiness, Piunan Publishing 1993.

trebuie să utilizăm mai bine informația și să ne dezvoltăm abilitatea de a dirija acțiuni mai bune.

Informația a constituit întotdeauna un aspect important al societății umane. Capacitatea de a comunica idei și concepte a fost considerată că fiind una din caracteristicile *homo sapiens*. Dezvoltarea mijloacelor de tipărire în Europa, datorită lui Gutenberg și Caxton, în secolul al XV- lea, a avut o influență profundă asupra educației și a lărgirii fundamentului intelectual, prin asigurarea unor surse de cunoștințe relativ ieftine și consistente unei audiențe mult mai mari, decât până în acel moment. De abia în a doua jumătate a secolului XIX s-a produs un nou salt, care a contribuit la îmbunătățirea mijloacelor de transfer ale cunoștințelor.

Apariția telefonului și a tehnologiilor transmisiilor fără fir, a permis transmiterea instantanee a informațiilor la distanță. Totuși, acest transfer de informații rămânea un proces linear și transparent prin care datele erau evaluate, după care informațiile analizate erau disponibile a fi transferate la utilizator, care putea astfel, să acționeze în consecință. Receptorul poate, dacă e necesar, să urmărească o revizuire a drumului parcurs pentru a evalua validitatea informației.

Așa, de exemplu, dacă în bătălia de la Waterloo, Wellington ar fi dorit să-și amendeze tacticile, ar fi scris noile sale ordine și le-ar fi înmânat comandantului potrivit pentru a le pune în aplicare. Dacă corpul mesagerului ar fi fost descoperit mai târziu cu sacul gol s-ar fi ajuns la concluzia că informația din mesaj a ajuns în mâinile francezilor.

Dacă prima jumătate a secolului XX a fost martora unui anumit număr de îmbunătățiri calitative a modului în care datele puteau fi transmise în lume, imperativele tehnologice ale celui de-al doilea război mondial au asigurat îndeplinirea viziunii lui Babbage: calculatorul și prin urmare, revoluția informațională.

Ca multe dezvoltări tehnologice, de-a lungul istoriei, forțele care s-au aflat în spatele inovațiilor acestei revoluții au fost aproape

exclusiv militare, reflectând prioritățile celui de-al doilea război mondial și pe cele ale războiului rece.

Marea schimbare a reprezentat-o faptul că factorii care determinau progresul acestor tehnologii se sprijineau mai puțin pe bugetele apărării sau pe alte resurse guvernamentale și mai mult pe priorități comerciale, aplicări și presiuni. Motivele acestei manevre sunt complexe, contribuind mult la stabilitatea și prosperitatea de care s-a bucurat Vestul în perioada războiului rece, dar și la abilitatea sferei comerciale de a dezvolta o piață globală și competitivă.

Termenul „revoluție" a fost utilizat, în ultimul timp, mai ales pentru a caracteriza dezvoltarea tehnologiei informaționale din ultimul deceniu. Dacă acum 50 de ani calculatoarele tindeau să automatizeze activitățile umane pentru a obține rapiditate și precizie, funcțiile acestora putând fi înlocuite de procese manuale, în schimb, sistemele moderne sunt interconectate și interdependente și nu mai pot fi considerate sisteme manuale.

Știinta și tehnologia ne promit că într-un viitor apropiat, sistemele de inteligență artificială vor realiza activități ce acum sunt îndeplinite de om. Doar un control uman limitat va fi necesar și majoritatea operatorilor se vor mulțumi să răspundă doar la ceea ce le vor cere software-uri sofisticate.

Există deja un număr important de implicații perturbatoare datorate dependenței de sisteme, mai ales la nivelul copiilor, care-și pierd capacitatea instinctivă de înțelegere și apreciere asupra problemelor matematice, când sunt prea preocupați de calculator. Aceștia așteaptă informațiile fără să le verifice validitatea. Și trebuie să ținem seama că acești copii vor fi managerii de mâine.

Într-un raport examinând doborârea avionului iranian Airbus 655 de catre USS Vincennes, în 03.07.1988, Rochlin [117] menționează câteva pericole ale dezvoltării instrumentelor

[117] Gene Rochlin, „Iran Air Flight 655 and the USS Vincennes", *Social Responses to Large Technical Systems*, Amsterdam Kluwer Academic publishers, 1991.

sotisticate, ale dispersării sistemelor centralizate de comandă-control, acestea devenind mai rigide și tot mai saturate de informație și responsabilități, fără a se înregistra vreo îmbunătățire a capacităților umane de a controla asemenea concepte.

Ar fi greșit să ne concentrăm exclusiv asupra noilor tehnologii ale revoluției informaționale. Tehnologia, chiar dacă este foarte sotisticată, reprezintă mai degrabă un instrument de manipulare a informației, care să pună cap la cap, să stocheze, să sorteze, să rafineze și să asambleze informațiile pe care le cere utilizatorul. Calculatoarele moderne pot stoca informațiile, le pot procesa și le pot distribui apoi în moduri nemaiîntâlnite până acum, făcând posibile mari beneficii în domeniul afacerilor, dar sporind și gradul și oportunitățile pentru un management defectuos, prin pierdere, neglijare sau diseminare discriminatorie a informației.

Informația, ca bun militar strategic, a fost întotdeauna recunoscută ca atare de către comandanți, mai ales în ideea unei bune cunoașteri a intențiilor adversarului și în același timp, a unei protecții proprii a planurilor și a stadiului operațional. Făcând această informație disponibilă în domeniul militar, de la nivelurile strategice de comandă la comandanți, apar o serie de probleme în privința încrederii acestora în integritatea, relevanța și validitatea informației prezentate. Distrugerea Ambasadei chineze din Belgrad de avioanele NATO constituie un exemplu al pericolului pe care-l prezintă acceptarea informațiilor fără a le veritica proveniența.

Extinderea revoluției informaționale la organizații, civile sau militare, nu a fost benefică tuturor. Strassman [118] considera că nu există o legătură directă între beneficiile acționarului și costurile pe care le suportă o firmă pentru tehnologia informațională. Această perspectivă este susținută de un studiu al revistei *The Economist* [119] care vorbește de introducerea electricității în

[118] Paul Strassman, „The Politics of Information Management-Policy Guidelines", *The Information Economic Press*, 1995.

[119] „What Computers are for", *The Economist*, 22.01.1994.

industria americană la începutul secolului XX, când beneficiile financiare începeau să apără, odată cu orientarea managerilor spre noile tehnologii.

Natura operațiilor militare și expunerea lor la o radiografiere permanentă a mass-mediei, va constitui o greutate în plus pe umerii decidenților militari, cu consecințe dramatice, în caz de insucces. Pentru a descoperi nevoile informaționale ale comandanților militari, este necesar să examinăm tipul activităților militare în care sunt angajați.

Există o diferență considerabilă între necesitățile informaționale cerute de operațiile de menținere a păcii, de exemplu, și cele cerute în timpul unui conflict major. Acest „spectru al conflictului" asigură un instrument analitic util și ne poate permite să distingem un anumit număr de legături comune.

Recentele operații din Kosovo, de exemplu, au scos în evidență cerințele pentru o capacitate de mișcare dintr-o parte a acestui spectru în cealaltă. Actuala operație de menținere a păcii poate degenera foarte repede într-un nou conflict.

O examinare fugară a sistemelor informaționale moderne dezvăluie faptul că instituția militară nu mai reprezintă motorul central al cercetării și dezvoltării tehnologiei. În momentul de față domeniul economic inițiază și conduce cercetările și dezvoltarea ei, într-o manieră nouă. Firmele comerciale își reconsideră sistemele informaționale pe care le înlocuiesc la intervale regulate de timp. Necesitățile militare și cele guvernamentale sunt stabilite mai degrabă pe zece ani și nu patru sau cinci ani cum procedează societățile comerciale.

În același timp, sistemele militare se interconectează tot mai mult cu cele din lumea civilă ceea ce ridică tot mai mult problema interoperabilității dintre aceste sisteme. Pe măsură ce presiunea asupra militarilor crește în privința inițiativelor de genul finanțării private, creării de agenții și pe măsură ce crește și nevoia unor legături mai strânse cu firmele civile, datorită dezvoltării și suportului lor, cresc și riscurile aferente unei asemenea interdependențe

Există un anumit număr de amenințări pe care le putem identifica, la adresa integrității informației.

Există trei parametri cheie pentru evaluarea naturii amenințărilor: identificarea autorului, a *modus operandi-ului* și a motivului.

Una din caracteristicile amenințărilor asupra informațiilor digitale este dificultatea identificării autorului. Sunt mai multe cauze care ar putea conduce la lansarea unui atac informațional:

- Un hacker care consideră o anumită rețea o provocare;
- Un angajat nemulțumit;
- Un criminal profesionist care încearcă să spargă sistemul de securitate pentru a obține un anumit profit;
- O companie națională sau multinațională care încearcă să obțină avantaje comerciale în dauna competitorilor săi;
- O organizație non-guvernamentală internațională care dorește să-și pună în aplicare planurile;
- Servicii secrete ostile, care încearcă să identifice și să exploateze punctele de vulnerabilitate ale unei alte țări, a infrastructurii sale militare și comerciale;
- Organizații teroriste care doresc să distrugă infrastructura socială, comercială sau militară a unui stat.

Modul de operare adoptat de autori variază, însă un instrument frecvent utilizat sunt virușii. Dezvoltați de către un profesor în matematică de la Universitatea din Sofia, aceștia sunt acum parte integrantă a domeniului calculatoarelor. Virușii continuă să afecteze lumea informațională, după cum s-a văzut și în prima parte a anului 1999 (Melissa, Cernobâl). Se estimează că aproape 200 de noi viruși sunt creați lunar [120].

Motivul atacului poate determina nivelul amenințării pentru o organizație și identifica acțiunile necesare pentru a neutraliza amenințarea. Pentru a examina motivul, trebuie să ne uităm la tipul atacului. Pe lângă atacurile intenționate, orice infrastructură informațională va fi vulnerabilă la nenumărate evenimente, iar o

[120] Stoll Clifford, *The Cuckoo's Egg*, London, Bodley Head, 1990.

protecție față de acestea se poate realiza chiar în sistem. Aceste evenimente includ dezastrele naturale.

O problemă mai serioasă este răspunsul dat la un act deliberat: acesta poate merge de la accesul neautorizat la furtul de informații, la distrugerea datelor, la inserarea de informații derutante în baza de date sau scoaterea din funcțiune a sistemului. Un astfel de exemplu este atacul asupra facilităților USAF de la Rome Air Development Center, din martie și mai 1994 [121]. Acest atac a compromis câteva sisteme, prin folosirea unor tehnologii care detectează identitatea și parola utilizatorilor.

Hackerul a utilizat mai multe site-uri localizate aparent în diferite țări (din Europa, America de Sud și Mexic) pentru a nu i se da de urmă. Când a fost în sfârșit prins de Scotland Yard, s-a constatat că acesta avea doar 16 ani și că trăia la Londra.

Capacitatea de a ascunde sursa atacului este una dintre caracteristicile tehnologiilor moderne, o formă de *„opacitate informațională"* care are multe implicații. Dacă un stat sau o organizație dorește să lanseze un atac împotriva altui stat sau organizație, acest lucru poate fi realizat prin intermediul unui al treilea stat sau organizație, dând impresia țintei că a treia parte este autorul real al atacului. Am aratat deja că împletirea și interconectarea sistemelor și un atac deliberat la adresa suportului infrastructurii, cum ar fi la nivelul legăturilor comunicațiilor, la sistemele din afara organizațiilor, la nivelul rapoartelor Reuters, a informațiilor comerciale sau a rapoartelor pentru logistica militară realizate pentru furnizori, pot avea consecințe serioase pentru organizație.

Granițele care delimitează orice organizație nu mai sunt impenetrabile ci permeabile informațiilor digitale. Acest lucru este luat în discuție mai jos, punându-se accentul pe problema suveranității naționale.

Orice strategie creată pentru a proteja informația strategică a unei organizații trebuie să examineze legăturile dintre propriile sisteme informaționale și cele exterioare.

[121] CSIS Report on Global Organised Crime.

Deși identificarea unui atac serios este greu de realizat, doar câteva atacuri sunt recunoscute ca atare de către utilizatorii sistemelor. Președintele SUA a cerut elaborarea unui studiu privind „Infrastructura Națională critică", iar în Marea Britanie Home Secretary a devenit responsabil pentru protecția comerțului electronic din UK [122].

Cum să protejăm sistemele militare sau civile când ele sunt interconectate cu altele? Pentru a putea evalua tipul necesar de protecție, câteva tehnici de management al riscului vor trebui să fie dezvoltate urmărind:

- Să identifice vulnerabilitățile informaționale din interiorul sistemului și între sisteme;
- Să identifice potențialele amenințări;
- Să clasifice amenințările;
- Să dezvolte strategii potrivite de recuperare.

Dezvoltarea strategiei potrivite de acoperire este un lucru foarte important. Din datele deținute de Departamentul American al Apărării reiese că există un număr mare de încercări de spargere a sistemelor militare și civile și că acest număr este în creștere ca urmare a interconectării existente și a creșterii gradului de sofisticare al instrumentelor utilizate de hackeri. Programul RI defensiv al SUA identifică trei faze de comportare: **protecție, detecție și reacție**.

Acest lucru permite sistemelor să fie protejate într-un mod cât mai practic, în timp ce sunt activate pentru a detecta intrușii într-un cadru organizațional de dorit, creat pentru a raporta spargerile și pentru a reacționa rapid, pentru a preveni viitoare atacuri, a ameliora pagubele și a restaura serviciile cât mai repede. Această activitate se concentrează asupra sistemelor din cadrul unei organizații și nu se interesează de vulnerabilitățile existente la nivelul sistemelor exterioare organizației.

Bineînțeles că nu este doar foarte costisitor să protejezi toate sistemele, dar nici nu e practic și, în consecință, în privința

[122] Declarația din Parlament a Home Secretary, 25.01.1999.

sistemelor care nu cer o securitate sporită, politica instituției trebuie să se concentreze asupra elementelor „detectare" și „reactie". Stabilirea siguranței informaționale potrivite are, deci, o importanță majoră și va cere pe viitor rutină și o riguroasă „revizie informațională".

Acestea vor fi similare cu cele care se realizează în cadrul organizației azi, pentru a monitoriza evaluările strategice, ca cele financiare și de personal. Revizuirea va urmări a examina ce informație e cerută de utilizator, de unde vine informația și cum e procesată.

Cine trebuie să fie responsabil de asigurarea securității informației? Să fie vorba doar de o competență tehnică sau de o funcție managerială? Consecințele căderii unui sistem pot fi atât de grave încât să-i afecteze pe toți membrii staff-ului unei organizații și deci responsabilitatea asigurării integrității informației le revine tuturor.

Managerii ar trebui să determine politica organizației pentru bunurile informaționale și să identifice cum aceasta poate fi măsurată și revăzută. Lista problemelor care trebuie luate în seamă cuprinde identificarea acelor bunuri, calitatea și cantitatea informației cerute și protejarea informației împotriva accesului neautorizat, de abuz sau de folosire greșită.

Organizațiile trebuie să examineze problema interconectării sistemelor și potențiala creștere a dependenței organizației de sistemele altei organizații. Un exemplu este cel al utilizării capacităților telefoniei comerciale pentru acoperirea nevoilor proprii unei organizații.

Deși utilizarea serviciilor ar trebui să presupună și asigurarea unor servicii acceptabile, vor exista tot mai multe motive pentru folosirea unei asemenea interconectivități în scopuri mai puțin onorabile. Acest lucru se întâmplă deja cu organizațiile conectate la Internet.

Devine limpede că problema integrității informației este una care afectează companiile, corporațiile multinaționale, guvernele

și, în cele din urmă, relațiile dintre state. Este instructiv să ne aplecăm asupra genezei conceptului război informațional, asupra relației dintre ethos-ul informației militare și elementele sale civile și să examinăm implicațiile asupra suveranității statelor-națiune.

Este clar ce înseamnă un „act de război" în cazul unui atac convențional, împotriva unui stat. Un astfel de atac va fi urmat de o declanșare a ostilităților, așa cum s-a întâmplat, de exemplu, după ce forțele argentiniene au invadat insulele Falkland, în aprilie 1982. O definiție asupra „războiului" a fost data de Malinowski (1968): „lupta armată între două unități politice independente, utilizând forțe militare, urmărind o politică națională sau tribală [123]. Atacurile germane asupra Londrei în cel de-al doilea Război Mondial sunt acoperite de această definiție. Aceste atacuri destinate distrugerii capacității Londrei de a funcționa ca un centru financiar și comercial, erau realizate de „forțe militare organizate".

Însă la un atac electronic, considerat act de război se poate răspunde la fel, dacă autorii nu sunt state-națiune, ci o instituție multinațională, de exemplu? Acesta devine o interogare intelectuală interesantă: dacă un stat nu poate spune ce e un război, sau să determine cine conduce un atac menit să provoace pagube, să distrugă importante bunuri naționale, cum ar fi orașul Londra, stabilitatea viitoare a statelor-națiune ar putea fi în primejdie.

În acest caz, cine, în cadrul statului-națiune trebuie să se ocupe de asigurarea unei apărări potrivite? Încă nu există o coerență la nivelul guvernului și a lumii economice în privința abordării problemei atacurilor realizate prin intermediul sistemelor electronice.

Termenul de „război" este peiorativ și aduce aminte de comentariul lui John Fowles [124]: „Bărbații iubesc războiul pentru că acesta le permite să pară serioși. Pentru că este sigurul lucru de care femeile nu râd de ei".

---

[123] *The Oxford Companion to Politics of the World,* Oxford University Press, 1993.

[124] John Fowles, The *Magus,* London Jonathan Cape, 1977.

S-au făcut progrese considerabile, în ultimii ani, despre cum războiul informațional poate constitui o nouă unealtă capabilă să atace societatea. Nu cred că e vorba de o nouă problemă, ci mai degrabă că a devenit mai insidios prin capacitatea de a culege mari cantități de informație și de a le disemina la nivel global. Discuțiile asupra războiului cibernetic și a războiului informațional se poartă in jurul ideii folosirii unor astfel de atacuri împotriva unui stat-națiune, ca alternativă la atacurile convenționale.

Acestea includ acele activități care nu corespund, în mod normal, normelor militare, dar care reflectă creșterea dependenței activităților guvernamentale și comerciale de diferite sisteme, vitale pentru funcționarea operațiilor militare moderne. Practic, de la un calculator anonim se pot cauza pagube considerabile la nivel politic, social, financiar, etc.

Sintagmele *Infrastructură Națională Informațională* (INI) și *Infrastructură Informațională Globală* (IIG) sunt destul de populare în SUA și reflectă natura organică și dinamică a rețelelor informaționale care s-au dezvoltat în sprijinul nivelelor de interconectivitate, dependență și integrare cerute. În ciuda numelor, nici INI și nici IIG nu există că sisteme integrate. Nu sunt proprietatea nici unei agenții sau companii, guvernul exercită o mică influență în procesul general de dezvoltare și sunt animate de cererile consumatorilor.

Aceste infrastructuri constau într-o multitudine de sisteme, de legături de comunicație și facilități. Există un flux continuu de informație la nivel global, volumul acestuia crescând exponențial pe măsură ce „infrastructura globală" continuă să se dezvolte. Vulnerabilitățile unor astfel de sisteme sunt numeroase, greu de identificat și nu pot fi evaluate corespunzător, datorită ritmului dinamic al schimbării și incapacității de a defini sistemul general.

În lumea occidentală, Londra își menține rolul de actor major în activitățile financiare și comerciale. Fluxurile informaționale sunt cheia succeselor sale: piețele financiare sunt acum controlate prin operații electronice globale realizate în timp real, care se ridică

la un cost de trei milioane £ pe an. Pagubele aduse companiei „The Baltic Exchange" datorită bombelor IRA, au produs disfuncții importante în activitățile comerciale ale Marii Britanii.

Activitățile unui singur comerciant din Singapore duce la decesul uneia dintre cele mai prestigioase bănci engleze, prin preluarea sa de către o bancă daneză. Beneficiile Marii Britanii în urma unor astfel de activități în Londra sunt considerabile și se reflectă în balanța de plăți națională. Este cert că un anumit număr de țări, instituții și corporații ar dori să vadă schimbat acest statut. E posibil ca pe viitor unii să se pregătească să precipite o astfel de schimbare, prin activități care să afecteze infrastructura informațională a orașului.

Blackstone a definit suveranitatea ca fiind „regula de acțiune prescrisă sau dictată care trebuie ascultată". Suveranitatea este un concept central a definiției statului-națiune. Din punct de vedere istoric, era considerată un concept secularizant, care reflectă declinul universal al autorității religioase, care încuraja ideea supremației statului asupra teritoriului său [125].

Pentru că nu există un super-stat care să controleze statul, fiecare stat e „suveran" în cadrul societății internaționale. La sfârșitul primului război mondial, președintele american W. Wilson a propus 14 puncte care reprezentau o încercare de îngrădire a suveranității naționale [126]. Acest proces a fost continuat de ONU care, deși este o organizație care asociază state suverane, își rezervă dreptul să intervină pentru implementarea măsurilor care să asigure pacea [127]. Acest lucru este evident în acțiunile întreprinse în Irak după războiul din Golf, ca și în cele din Iugoslavia, în care ONU și NA TO au intervenit într-o problema națională.

---

[125] A se vedea *Oxford Companion to Politics of the World,* Oxford University Press, 1993.

[126] Hugh Brogan, *History of the United States of America,* Longman, London 1991.

[127] Peter Calvocoressi, *World Politics since* 1945, Longman, London 1991.

În Europa, dezvoltarea Uniunii Europene a necesitat un transfer de suveranitate către Bruxelles, în anumite domenii. Ceea ce e numit atât de des „suveranitate națională" poate fi considerat, în realitate, ca fiind compus din mai multe straturi: *suveranitatea etnică,* în care puterea politică rezidă doar în mâinile unor cetățeni aparținând unui grup etnic, *suveranitatea lingvistică,* în care puterea aparține celor care posedă anumite priceperi lingvistice și *suveratitatea culturală,* în care caracteristicile unui stat-națiune sunt definite în termenii moștenirii sale culturale și un atac asupra acesteia este considerat a fi un atac la suveranitatea statului însuși. Acest lucru se poate vedea în cazul Franței, în care guvernul a făcut eforturi considerabile pentru a stopa importul culturii americane.

Un alt element al suveranității naționale este *suveranitatea informațională,* în care un stat-națiune tinde să controleze fluxul informațional în cadrul statului și în afara granițelor sale. O consecință a revoluției informaționale a constituit-o creșterea inabilității statului de a controla fluxul imaginilor și ideilor, care modelează gusturile și valorile umane.

În ceea ce privește conceptul de *ciberspațiu,* este evident că noțiunea de *frontieră* devine irelevantă din ce în ce mai mult. Cum pot statele să asigure integritatea sistemelor lor? Pot să insiste asupra standardelor minime ale comportamentului etic al cetățenilor lor, în privința materialelor disponibile gratuit, sau va fi vorba de o gratuitate pentru toți?

Globalizarea infrastructurii informaționale repune în discuție conceptul de stat-națiune, în cazul în care, de exemplu, o organizație, care își desfășoară activitatea într-o anumită țară are aceleași viziuni politice ca cele ale unei alte țări.

Paul Kennedy credea că: „adevăratul motiv al existentei unei frontiere este ca nimeni să nu aibă controlul absolut, cu excepția, poate, a managerilor corporațiilor multinaționale, a căror responsabilitate este îndreptată către acționari, care, se poate spune că au devenit noii suverani, și investind într-o companie, dau cele mai mari profituri" [128].

Conceptul de suveranitate se află, de aceea, sub o mare

[128] Paul Kennedy, *Preparing for the Twenty-First Century,* New York, Vintage Books, 1994.

presiune și nu mai corespunde dezvoltării globale a infrastructurilor informaționale.

Rolul informației în zilele noastre nu e foarte diferit de cel pe care-l avea în trecut. Avem nevoie de informație pentru a putea lua decizii, pentru a interacționa social și pentru a trăi. Ceea ce s-a schimbat, totuși, este natura cantitativă a informației și, după cum remarca Stanislaw Lem, un filosof polonez, „timpul marilor politicieni a trecut pentru că fluxul informațional face imposibil, prea complicat procesul decizional"[129].

Problema integrității informației, când se confruntă cu un astfel de flux informațional, devine critică și decidenții trebuie să știe care informație e validă, care e coruptă, care e relevantă și care ar trebui ignorată. Procesarea modernă a informațiilor, după cum am văzut, e vulnerabilă și informația poate fi coruptă, distrusă sau modificată în timpul ei.

Ritmul schimbărilor tehnologice pare să nu încetinească și multe din problemele ridicate aici vor trebui abordate în viitorul apropiat dacă vom dezvolta calitățile necesare, modelele și metodologiile care să fie capabile să cuantifice amenințările la care sunt supuse sistemele.

Consecințele ignorării acestor probleme vor fi foarte mari. Acestea trebuie să devină un subiect de reflecție pentru întreaga societate și nu doar a unui singur grup concentrat asupra problemelor tehnologiei informaționale. Spectrul cunoașterii poate fi foarte folositor.

Ne-am concentrat atenția în acest material asupra informației, fluxului informațional, integrității informaționale și managementului informațional. Însă ce va trebui să facem de acum încolo este să ne aplecăm asupra procesului prin care această informație este utilizată de creierul uman. Este posibil să fim asistați în acest proces de inteligență artificială și de tot ceea ce ar putea urma acesteia. Trebuie să încercam să răspundem la dificila întrebare: cum putem face să restabilim abilitatea factorilor de decizie din oricare domeniu de a lua decizii, bazându-se pe un grad de confidență, de integritate și de relevanță a informației?

[129] Stanislaw Lem, *The Times Magazine*, 11.05.1996.

ANEXA 1

NETWORK CENTRIC WARFARE
– Un concept controversat –

Netwok Centric Warfare

NCW se fundamentează pe experiența acelor organizații care s-au adaptat cu succes la presiunile exterioare intrinseci Erei Informaționale. Studierea conceptului de Network Centric Warfare ne conduce la o concluzie majoră, și anume aceea că **adaptarea presupune schimbarea metodelor.**

NCW recunoaște importanța informației, potențialul de putere al acesteia. Acest potențial este rezultatul direct al relaționărilor inter-individuale, inter-organizaționale și al proceselor dezvoltate de aici. Aceste noi tipuri de relații creează noi tipuri de comportamente și moduri de operare.

NCW furnizează o nouă perspectivă de analiză a misiunilor militare, a operațiilor și a organizațiilor, centrată pe găsirea **soluțiilor inteligente** prin depașirea ideilor preconcepute.

Acest capitol începe prin a defini și explica **fundamentele conceptuale** ale NCW.

Capitolul include și o vedere generală prin prisma NCW asupra entităților care acționează în câmpul de operații.

Definiția NCW

Conceptul se definește prin referirea la oameni și organizații pornind de la **necesitatea adoptării unei paradigme noi** (gândirea *network centric)* și aplicarea ei în sistemul operațiilor militare.

NCW se centrează asupra puterii de luptă care poate fi generată prin eficientizarea legăturilor dintre diferite structuri de luptă. Principala sa caracteristică constă în abilitatea de dispersare geografică a forțelor în scopul cunoașterii partajate a câmpului de luptă.

NCW sprijină comanda rapidă, convertirea informației superioare în decizie.

NCW este transparent la misiune, mărimea forței, și factorii geografici. Mai mult, dispune de potențial permițând fuzionarea nivelelor tactic, operațional și strategic.

Pe scurt, NCW nu se limitează doar la aspecte tehnologice, ci la întregul spectru de probleme pe care le poate presupune războiul în Era Informațională.

Ca întreprindere de tip NCW, armata corelează elemente de bază necesare generării puterii de luptă. Ca și în sectorul economic totul începe de la Infrastructura Informațională. Aceasta oferă posibilitatea cunoașterii **partajate** a câmpului de luptă. Această „cunoaștere" constituie **pârghia** pentru sincronizarea forțelor și pentru comanda eficientă.

Efectul îl reprezintă accelerarea ritmului operațiilor.

Pentru definirea conceptului trebuie să lămurim câțiva **termeni-cheie:**

1. „**Dispersarea geografică a forțelor**". În trecut se limita la:
   – abilitatea de a comunica;
   – de mișcare;
   – de protejare a forțelor și a elementelor lor de sprijin aflate în locațiile lor sau în imediata vecinătate a inamicului.

De aceea „dispersarea geografică a forțelor" era destul de slabă și nu putea răspunde rapid în cazul atacurilor concentrate. Tehnologiile specifice erei informaționale fac posibilă eliberarea puterii de luptă din locațiile fizice ceea ce va conferi forțelor o mobilitate eficientă. Eliminarea constrângerilor geografice asociate cu lupta prezintă următoarele avantaje:

a. Permite trecerea de la abordarea bazată pe comasarea trupelor la cea bazată pe efectele de luptă.

b. Nu mai este necesară concentrarea forțelor deoarece abilitatea de comunicare a informațiilor este extrem de rapidă și nu mai este limitată de constrângerile geografice.

c. Permite ștergerea urmelor reducând astfel riscul de a fi descoperiți de adversar. Conceptul de ***manevră*** se extinde prin reducerea nevoilor de transport a obiectelor fizice, consumatoare de bani și de timp.

Cu NCW putem avea același lucru în mai multe locuri și la momente diferite. Aceasta pentru că un anumit senzor se poate afla într-o poziție care vizează mai multe ținte fără să fie deplasat.

2. **„Intelligent"**. Acest termen desemnează puterea dată de deținerea informației, derivată din partajarea cunoștințelor despre câmpul de luptă și înțelegerea intențiilor comandanților, din sincronizarea proprie, din ștergerea urmelor.

O forță inteligentă se bazează pe informație oportună și viabilă precum și pe existența instrumentelor de procesare și expertiză necesare.

3. **„Legături eficiente"** între entitățile aflate în câmpul de operații. Aceasta presupune:

a. Entitățile dispersate și distribuite care pot genera sinergie

b. Responsabilitățile și munca care le poate dinamiza în scopul adaptării la situații. „Legăturile eficiente" necesită existența unei infrastructuri informaționale robuste care să furnizeze tuturor elementelor acces la informație. Mecanismele și procesele care creează aceste „legături eficiente" determină coeficientul de putere și de multiplicare. Natura legăturilor care furnizează cea mai bună performanță pe tot spațiul de operații constituie o problemă foarte importantă. Scopul este acela de a construi o configurație care să asigure eficiența forțelor.

Așa cum a fost definit mai sus, NCW reprezintă cel mai adecvat termen care poate descrie **evoluția cea mai probabilă** a conceptului de ***război*** în **Era Informațională**.

NCW recunoaște natura dinamică și complexă a războiului. NCW oferă comandanților o nouă abordare, mai flexibilă. Flexibilitatea operațională va putea răspunde provocărilor Erei Informaționale.

Conceptul de NCW nu presupune, așa cum cred greșit unii, numai comunicarea prin intermediul rețelelor de computere. NCW reprezintă un mijioc pentru atingerea unui scop.

El face legătura dintre diferitele state majore aflate în spații geografice diferite. NCW nu se concentrază pe tehnologie ci pe fluxul informațional, pe natura entităților aflate în spațiul de operații și pe interacțiunea dintre ele. NCW reflectă și încorporeaza caracteristicile necesare pentru eficiență în Era Informațională.

Puterea NCW

NCW se centrează pe avantajele oferite de partajarea informațiilor privind câmpul de operații, caracteristică ce reiese din însuși titulatura termenului. Aceasta permite obținerea efectelor sinergice. NCW este construit în jurul conceptului de **„partajare a informațiilor"**, „punere în comun a informațiilor". Doar rețeaua face posibilă o astfel de partajare *(sharing)*.

O rețea constă în noduri și legăturile dintre noduri. Nodurile constau în lucruri (decizii, acte) și informații.

Legătura dintre entitățile aflate în câmpul de operații vor determina creșterea eficienței operațiilor. Experiența din sectorul civil ne-a arătat în ce mod materia poate fi substituită cu informația și cum, fără să miști oameni, poți deplasa numai informații. Acestea duc la reducerea resurselor materiale și de timp.

Pentru a înțelege NCW trebui să vedem **în ce mod operează nodurile** în legătură cu o țintă. Pentru aceasta se execută următorii pași:

- Detectarea țintei;
- Identificarea țintei;
- Decizia de a ataca ținta;
- Transmiterea deciziei;
- Lansarea armei și deschiderea focului asupra țintei.

Pentru acestea trebuie stabilite: timpul și nivelul de luptă.

- **Timpul** se stabilește în funcție de următorii factori:

1. gradul de mobilitate a țintei,
2. contramăsurile adoptate de țintă,
3. natura senzorilor și a armamentului,
4. gradul de procesare a informațiilor,
5. procesul decizional.

- **Nivelul de luptă** se stabileste în funcție de:

1. caracteristicile senzorilor și armelor,
2. de consumul de timp pe care îl presupune.

În operațiile de luptă performanța capabilităților combinației dintre senzori și armament este în primul rând guvernată de învelișurile platformei centrice de angajare create numai atunci când platformele având la bord senzori asigură o calitate a

cunoașterii. Pentru luptători, ținta este în cadrul învelișului de angajare maxim al armamentului.

Un înveliș efectiv de angajare este zona definită de suprapunerea parțială a calității cunoașterii și învelișul care reprezintă implicarea maximă a armamentului.

Ca urmare puterea de luptă instantanee pentru ca o platformă centrică să fie angajată este proporțională cu învelișul de angajare efectiv.

În operațiile NCW puterea de luptă este adesea limitată de către inabilitatea platformei de a genera o cunoaștere de calitate care să fie folosită la angajarea acțiunilor într-o măsură mai mare sau egală decât maximum învelișului de angajare a armamentului.

Această situație apare frecvent în angajamentele platformelor NCW din luptele aeriene ca rezultat al inabilității unui echipaj al unei aeronave de a identifica rapid și eficient dacă mijloacele aeriene care îl înconjoară sunt amice sau inamice și dacă ceea ce descoperă și urmărește este ca atare detectat de senzori.

În marea majoritate a operațiilor luptătorii, trăgătorii, sunt angajați în conjuncție cu capabilitățile de comandă și control. Situațiile operaționale care există atunci când o platformă centrică de tragere este legată de un nod de comandă și control cu capabilități de senzori prin intermediul unor legături prin voce pot fi în practică diferite. Nodul de comandă și control este capabil să dezvolte un nivel al cunoașterii situației limitat, bazat pe informațiile asigurate de către senzori care pot să fie dispuși în cadrul nodului C2, sau extern.

În cele mai multe situații nivelul de cunoaștere disponibil al nodului C2 este calitativ suficient pentru a conduce un trăgător într-o zonă de angajare, dar insuficient pentru a-i permite trăgătorului să fie dirijat direct.

Mai departe, câtă vreme legătura dintre platformele C2 și platforma centrică de tragere este o legătură prin voce, tot schimbul de informații dintre acestea trebuie să aibă loc tot prin voce.

Pentru exemplu, în lupta de combatere a operațiilor aeriene, ofițerul cu armamentul aflat la bordul unei aeronave E - 2 Hawkeye sau al unui E - 3 AWACS, nu trebuie să aibă în mod necesar o

calitate anume a cunoașterii pentru a angaja acțiunile contra tuturor obiectelor care sunt urmărite.

În mod tipic, fiecare incertitudine asociată poziției unei ținte potențiale este mare, sau informația disponibilă este insuficientă pentru a identifica în mod cores-punzător o țintă.

În consecință echipajul unui avion de vânătoare trebuie să aibă senzori la bord care să asigure o cunoaștere a situației de calitate și care să permită și acțiunea, respectiv executarea atacului cu armamentul din dotare.

Mai mult, câtă vreme toate informațiile schimbate au loc prin voce, poate fi extrem de dificil pentru echipele din nodul C2 și platformele de tragere să dezvolte și să mențină o cunoaștere a situației atunci când există un număr mare de mijloace ale forțelor albastre sau roșii care operează într-o zonă apropiată.

Prin comparație operațiile de rețea centrică din NCW, capabilitățile de sesizare, de comandă, de control sau de angajare sunt strâns legate și lucrează în rețea prin intermediul datelor digitale. Sursa acestei puteri sporite în operațiile de rețea centrică derivă în parte din conținutul sporit, calitatea și oportunitatea fluxurilor de informații dintre noduri în cadrul rețelei.

Această sporire a fluxului de informații este esențială pentru a permite partajarea cunoașterii situației din câmpul de luptă și pentru sporirea acurateței informațiilor .

Experiența operațională cu date, cu legături digitale, de nivel tactic, dovedește puterea operațiilor în rețeaua centrică.

Într-un experiment care a comparat performanța operațională a lui F15 îndeplinind o operație de luptă aeriană cu și fără legături de date, forța aeriană a descoperit cum prin întrebuințarea rețelelor NCW **coeficientul de letalitate sporește ajungând până la 100%.**

Această putere de luptă sporită a rezultat din semnificativa sporire a cunoașterii situației din spațiul de luptă care a fost asigurată piloților care au operat cu **date de legătură tactice.**

Componentele cunoașterii situației din câmpul de luptă includeau performanța armamentului forței albastre (un exemplu), poziționarea în timp real a albaștrilor și forțelor roșii, starea, situația, acțiunilor, în desfășurare a albaștrilor.

Rezultatul evident a fost o îmbunătățire semnificativă a capabilităților de a observa, orienta, decide și acționa. Constatările recente ale echipei de evaluare și identificare a serviciului de luptă au confirmat toate acestea.

De exemplu o situație "A" care prezintă două platforme centrice de tragere ce operează în proximitate susținute de senzori externi care pot să asigure informații specifice.

Într-o astfel de situație informația despre acțiunile desfășurate în timp real nu poate fi partajată efectiv iar puterea de luptă nu este maximizată.

Prin contrast în situația "B" valoarea adăugată a puterii de luptă asociată cu o operație NCW. În acest mod de operare o partajare a informației aproape în timp real între noduri, dezvoltă mult puterea de luptă.

Lucrul fiabil în rețea, al senzorilor asigură forței capabilitatea de a genera o cunoaștere partajată mărind în același timp și calitatea. Această cunoaștere sporită este proporțională cu întreaga zonă acoperită de către senzorii zonali, putând fi exploatată de către un fiabil lucru în rețea al C2 și de către entitățile, actorii din zonă, care pot astfel să coopereze, și să-și autosincronizeze forțele.

Potențiala sporire a puterii de luptă în ansamblu, asociată cu operațiile NCW este dată de mărirea suprafeței învelișului de acțiune efectivă.

Nu putem păstra forma simplă a lucrurilor din întregul spațiu de luptă fără o organizare corespunzătoare și fără schimbări doctrinare care să mărească eficiența în desfășurare a acțiunilor de luptă.

Practic, există consecințe neintenționate ale conectării spațiului de luptă și în speranța de mai bine, de fapt putem degrada performanța în mod particular dacă schimbăm neadecvat doctrina, organizarea, instruirea și alte elemente cheie ale procesului.

De aceea drumul către un război bazat pe NCW are nevoie să fie îmbogățit cu analize și experimente în scopul de a înțelege cum putem beneficia cât mai mult de pe urma potențialului imens al NCW în timp ce evităm consecințele neintenționate.

Măsura în care productivitatea lucrului în rețea depășește suma productivității părților sale depinde de două lucruri.

Primul este câștigul și poate fi obținut prin simplă partajare a resurselor (informației) din cadrul nodurilor.

În mod evident nu toate organizațiile au probabilitate egală de a avea informațiile de care au nevoie.

Aceasta la momentul de față lucrează în favoarea noastră, pentru că noi folosim cunoștințele despre organizațiile și indivizii care sunt cel mai probabil în măsură să-și obțină informațiile care le trebuie.

Având dezvoltate aceste capabilități, puncte de comandă și informații inteligente pentru planuri, putem, folosind puterea lucrului în rețea să transformăm o probabilitate foarte scăzută de a avea o infor-mație într-una foarte mare.

Acesta este practic aspectul la care se gândesc cei mai mulți oameni atunci când se referă la puterea lucrului în rețea, dar este totodată vorba și de o nouă ipoteză fundamentală care sugerează că deblocarea întregii puteri a lucrului în rețea implică afectarea naturii deciziilor care sunt în mod inerent făcute prin intermediul rețelelor.

Aceasta poate să nu fie imediat distinctă câtă vreme aceste decizii colective sunt adesea implicite și de aceea nu tocmai vizibile.

Este necesar să acordăm mai multă atenție comportamentului entităților care lucrează în rețea, mai curând decât să studiem și să considerăm comportamentul entităților individuale. Rezultatele Flotilei Delta de Luptă Experimentală, oferă suport pentru aceste ipoteze.

Este axiomatic aproape pentru orice situație că putem de fiecare dată să facem în așa fel încât, măcar până la limita constrângerilor să fie bine, să ne îmdreptăm spre succes.

Cu toate acestea, nu de puține ori constrângerile sunt folosite ca mijioace de a obține rezultate care adesea sunt importante obiective ale sarcinilor primite.

De exemplu, ne referim la niște actori însărcinați să atace un număr de ținte.

Costrângerile asupra opțiunilor sunt adesea folosite ca mijioace de a reduce fratricidul chiar dacă vor reduce probabil și

numărul de ținte doborâte și vor mări riscul ce 1-ar presupune pierderea secretului acțiunilor.

Scopul NCW în această situație este de a obține o reducere a probabilității de fratricid, concomitent cu minimizarea constrângerilor cu privire la folosirea armamentului.

O modalitate de a reuși acest lucru este de a face actorii să fie mult mai înștiințați, informați, iar armamentul acestora tot mai inteligent.

În operațiile de luptă capacitățile performante ale armelor cu senzori sunt guvernate de teren, de "argumente geometrice" (Platform-Centric Engagement Envelope

Astfel:

1. un factor de decizie fără constrângeri (limitări) informaționale.

2. câțiva factori de decizie, fiecare cu viziuni limitate și cu informații procesate limitate.

Hai să luăm în considerare cazul când un singur decident poate cunoaște informațiile comune despre țintă, în sensul că deține tabloul complet al câmpului de operații și timpul necesar procesării și transmiterii ordinelor fiecărui actor implicat.

În aceste condiții decizia optimă poate fi influențată. În astfel de cazuri funcția rețelei este aceea de a contribui la creearea unui tablou complet prin asamblarea descrierilor parțiale și de a transmite aceste informații (cunoștințe) de la factorii de decizie către fiecare actor implicat.

Cu alte cuvinte nodurile senzori, partajează fiecare informațiile lor cu nodul decizional, care la rândul lui partajează decizia cu actorii implicați în fiecare nod. Totuși în viața reală acest lucru este puțin probabil să se producă așa de eficient.

Rareori se pot lua decizii optime. Pentru oricine decizia optimă centralizată reprezintă un obiectiv foarte greu de atins.

Pentru NCW lucrurile nu stau deloc așa.

Observăm că puterea NCW derivă din împuternicirea tuturor factorilor de decizie nu doar a câtorva. Dimensiunile complexe și ritmul operațiilor trebuie să ne conducă în cele din urmă la utilizarea rețelelor.

Obiectivul este acela de a implica toți actorii în același tip de joc și la timpul oportun. În ceea ce privește controlul, NCW nu conduce automat la controlul centralizat.

Pe de o parte NCW amplifică cunoașterea pentru toate entitățile implicate, pe de altă parte duce la descentralizarea deciziei și a controlului. După cum se aplică NCW în managementul informațional al câmpului de operații ne putem aștepta, în termeni absoluți, că fiecare entitate va deține mai multe informații despre acesta.

În viitor ne putem aștepta ca la nivel tactic comandanții vor avea o mai bună înțelegere asupra caracteristicilor câmpului de operații și a necesităților de instruire.

Colaborarea virtuală

În acest capitol vom examina natura beneficiilor ce pot fi obținute prin partajarea informațiilor și bunurilor. Mai devreme ideea a fost aceea că un lucru robust în rețea al ecosistemului de ducere a acțiunilor de luptă permite unor lucruri și sisteme de relații noi să se dezvolte.

Un astfel de produs, dintre cele mai puternice, care rezultă într-un asemenea câmp de luptă este colaborarea virtuală.

Colaborarea virtuală este mai mult decât simpla partajare a informațiilor; ea permite elementelor unui ecosistem de ducere a acțiunilor de luptă să interacționeze și să colaboreze în domenii virtuale, să „miște" informația în loc de a „mișca" oamenii și să obțină un nivel de cunoaștere critic în rândul maselor.

Compo-nentele tehnologice cheie cum ar fi videoteleconferința și aplicațiile de planificare colaborative permit o colaborare virtuală. Colaborarea virtuală în domeniul informațional are numeroase beneficii operaționale.

De exemplu, o colaborare virtuală permite timpului asociat procesului de planificare și executare existent să fie mult mai redus. Aceste economii, ulterior, înseamnă timp suplimentar pentru executarea unor antrenamente, deplasări la contact sau odihna trupelor. Rezultatul final se regăsește în sporirea eficienței.

În operațiile expediționare aerospațiale „mișcarea" informației în locul oamenilor schimbă mult dinamica forței și proceselor desfășurate permițând derularea unor operații independente. Conceptul s-a dovedit promițător de exemplu în timpul Forței Expediționare Experiment '98.

Operațiile independente pot reduce atât timpul necesar pentru a iniția operația aeriană, cât și pentru a rentabiliza transportul aerian pentru a deplasa capabilități de luptă în teatru.

Abilitatea de a „mișca" informația în locul luptătorilor are totodată beneficii semnificative și în alte domenii.

Cunoașterea Câmpului de Operații

NCW dezvoltă și menține capacitățile de cunoaștere a caracteristicilor câmpului de operații prin colectarea, procesarea și diseminarea informațiilor.

Aceasta presupune partajarea și fuzionarea informațiilor într-un așa numit COP sau altfel spus ***(Common Operational Picture)***

Furnizarea către trupele întrunite a cunoștințelor oportune și viabile despre spațiul de luptă presupune colectarea datelor și informațiilor din surse multiple, procesarea în care este inclusă și analiza, transportarea, fuzionarea, plasarea în context și prezentarea în modul cel mai adecvat.

De asemenea, este necesară instruirea în acest sens a entităților și actorilor implicați în procesul decizional.

În concluzie, putem observa că NCW preupune atât cunoașterea spațiului de operații cât și a modelelor cognitive care permit această cunoaștere.

Informații incluse într-un astfel de tablou reprezentativ al câmpului de operații pot fi următoarele:

- **Locația** (pozițiile curente, gradul de mobilitate, predicții legate de pozițiile viitoare);
- **Statutul** (gradul de operabilitate, capacitățile de luptă, susținerea logistică, etc.);
- **Cursul** acțiunii actuale și predicția celei viitoare a inamicului(capacitățile ofensive și defensive ale adeversarului, evaluarea pagubelor, etc.);

• **Mediul** (condițiile atmosferice actuale și viitoare, efectul vremii asupra operațiilor, caracteristicile terenului cum ar fi gradul de circulare, liniile de vizibilitate, etc.)

Partajarea acestor informații presupune accesul tuturor forțelor la Tabloul Operațional Comun. Informațiile despre spațiul de operații trebuie considerate ca o proprietate comună (un fel de **conștiință colectivă**). Ea trebuie să funcționeze nu doar în cadrul unui nod, ci în toate nodurile relevante din toate eșaloanele și componentele funcționale.

Conținutul informațiilor din tabloul operațional necesare factorilor de decizie poate varia în funcție de eșaloane..

Partajarea cunoașterii situației din câmpul de luptă apare atunci când elemente relevante ale ecosistemului de ducere a războiului sunt asigurate cu acces la COP (imaginea comună operațională).

Practic, cunoașterea situației din spațiul de luptă trebuie să fie văzută ca pe o proprietate colectivă. Nu există numai un singur loc (nod) în spațiul de luptă, și mai mult, toate nodurile din spațiul de luptă din cadrul eșaloanelor sau din cadrul componentelor funcționale pot fi relevante. Gradul de detaliere care este ilustrat în imaginea operațională comună poate să fie însă diferit de la eșalon la eșalon.

Gradul în care conținutul informației dintr-un cadru operațional poate să varieze în funcție de eșalon. Informația pentru a genera cunoașterea situației din spațiul de luptă va fi asigurată din numeroase surse.

De exemplu, informația din cadrul forțelor roșii poate să fie culeasă prin intelligence, supraveghere și platforme de recunoaștere care operează ca parte a senzorilor de rețea, senzori angajați în platforme de armament, sau oamenii, agenții din teren (trupele de cercetare).

O partajare a cunoașterii pozițiilor albaștrilor în cadrul spațiului de luptă poate să fie generală prin permiterea tuturor elementelor forțelor albastre de a transmite informații despre poziții actuale și de a recepționa informații despre poziții relevante cu privire la alte entități.

Fiecare element al forțelor albastre poate să stabilească poziția sa în spațiul de luptă cu un mare grad de precizie prin folosirea sistemelor de navigație specifice cum ar fi **sistemul de poziționare global (GPS).**

Despre situația forțelor albastre, cum ar fi situația carburanților sau performanța armamentului, aceasta poate să fie generată prin folosirea unor senzori încastrați, sau de teren, care să urmărească de pildă consumul de carburanți sau efectele artileriei.

Operarea cu date în timp aproape real poate fi de asemenea luată în calcul, contribuind la menținerea dinamicității sau a gradului de operativitate la nivel operațional prin stabilirea cu anticipație și precizie a unor nevoi de întreținere.

Mediul informațional poate fi conectat prin diferite tipuri de senzori tradiționali cărora să le fie sporit potențialul prin informațiile primite de la senzorii de pe platformele de armament.

Generarea de cunoaștere a situației partajată a albaștrilor necesită un mecanism în locul „capturilor" de dinamicitate, poziție, situație sau informații, despre intenția sa de la toate elementele forțelor albastre și să avem capabilitatea de a asigura informații relevante doar pentru albaștrii care au într-adevăr nevoie de ele.

Pentru ca aceasta să se întâmple, toate elementele relevante ale forțelor albastre au nevoie să fie participante la proces.

Ele au nevoie să fie conectate în rețea.

În scopul de a obține o cunoaștere a situației din spațiul de luptă și apoi de a obține o avertizare asupra acestuia avem nevoie să trecem dincolo de informațiile care ne spun de locul lucrurilor și să ajungem la acele informații care ne dezvăluie și identitatea lor.

Este de asemenea necesar să cunoaștem câte ceva despre situația operațiilor în desfășurare, cum la fel de important este să știm despre doctrină și intenții.

În mod similar dacă informațiile despre forțele roșii, sau aspectele ce țin de situația acesteia, sunt obținute de o componentă a forței, pentru a genera o cunoaștere a situației din spațiul de luptă este necesară distribuirea lor, tuturor elementelor relevante ale forței.

Abilitatea de a dezvolta surse de informații precise și oportune pentru cunoașterea situației din spațiul de luptă depinde de caracteristicile proceselor informaționale disponibile și de performanța rețelelor.

De exemplu precizia unei informații de poziție distribuită cu privire la niște ținte mișcătoare (amice, neutre sau roșii) este în funcție nu doar de procesele de colectare și analiză ci de asemenea și în funcție de viteza de deplasare a obiectivelor sau de viteza informațiilor din cadrul rețelelor albaștrilor.

De exemplu o platformă de armament a albaștrilor cum ar fi un AH 64 D Apache detectează o coloană de tancuri.

Senzorul aflat la bord este capabil să genereze o informație de calitate cu privire la acțiunea în sine și nu neapărat de o detaliere care să indice și numărul de tancuri inamice din respectiva coloană.

Această informație are o valoare potențial semnificativă pentru forța care luptă.

Valoarea acestei informații este în funcție de posibilitatea de a o partaja și cât de oportun se face partajarea.

De exemplu dacă Apache-ul poate să ofere o cunoaștere de calitate a acțiunii în care sunt antrenați militarii unei baterii de artilerie într-un timp real atunci există posibilitatea pentru forțele albastre de a comasa efectele focului direct cu cele ale focului indirect.

Dacă informația nu poate fi transmisă în timp real atunci oportunitatea de a comasa efectele este pierdută. Cu toate acestea dacă informația despre o poziție a unei ținte colectată de către un Apache poate fi transmisă, dar nu în timp real, informația trebuie să fie suficient de precisă pentru a permite un sprijin aerian apropiat, respectiv atacarea acelei coloane de tancuri.

În mod similar dacă un comandant dorește să sporească viteza manevrei forțelor sale, menținând în mod simultan cunoașterea situației din spațiul de luptă atunci viteza informației trebuie să crească odată cu viteza manevrei.

De exemplu putem observa că după cum viteza medie a forțelor albastre crește, precizia informațiilor de poziție partajate va descrește dacă viteza medie a informației nu sporește în mod corespunzător.

Aceasta apare din cauza **preciziei instantanee** care este o **funcție a latenței informației**. În mod simplificat folosind o rată constantă de actualizare a poziției, eroarea instantanee de poziție a unei platforme de armament care se deplasează cu 500 de mile/ oră, cum ar fi viteza unui avion, este potențial de 10 ori mai mare cum ar fi cea a unei platforme care se deplasează cu 50 de mile/ oră, cum ar fi viteza unui tanc.

În rezumat, precizia, acuratețea, unei informații într-o imagine operațională comună este în funcție de :

- exactitatea sursei de informații,
- viteza informațiilor dintre nodurile din rețea
- viteza țintelor în cadrul operațional comun.

Abilitatea noastră de a asigura entităților din spațiul de luptă accesul la informație poate să fie exploatată pentru a spori acuratețea sau precizia informațiilor noastre despre bunurile inamicului.

Particularitățile despre cum o creștere a vitezei informațiilor poate fi folosită pentru a spori cunoașterea situației din spațiul de luptă este tratată mai jos.

Network Centric Warfare și Funcțiile de Comandă-Control și execuție

Am văzut în capitolele anterioare că adoptarea și implementarea conceptului de NCW determină o creștere semnificativă a abilității de cunoaștere partajată a câmpului de operații.

În următorul capitol se pune accentul pe implicațiile NCW asupra funcțiilor de execuție și comandă-control.

Natura funcției C2 constă în capacitatea comandantului de a înțelege și controla orice situație. În acest scop comandanții sunt instruiți cu acele cunoștințe necesare exercitării funcției de C2.

Out-put-urile funcției de comandă-control constau în:

1. **decizii** adoptate în funcție de percepția comandanților asupra situației și de intențiile lor;
2. **executarea deciziilor.**

Acest capitol se centrează pe **relația** dintre partajarea

informațiilor prin intermediul NCW, eficiența deciziilor și a implementării lor. Folosind conceptele tipice NCW se poate obține un grad foarte înalt de cuplare între C2 și controlul focului.

Această cuplare strânsă care permite translatarea până la cele mai înalte nivele a informațiilor partajate despre câmpul de operații generează creșterea puterii de luptă. Aceasta poate fi obținută prin multe modalități: planificarea și execuția, operațiile de distrugere, sincronizarea operațiilor. Astfel de exemple vor fi prezentate pe parcursul acestui capitol.

NCW furnizează oportunități de îmbunătățire a funcțiilor C2 și de execuție la nivelul fiecărui eșalon în contextul misiunilor specifice deoarece:

- Entitățile decizionale sau elementelor specifice C2 vor deține mai multe cunoștințe;
- Actorii implicați vor deține mai multe cunoștințe;
- Actorii și entitățile decizionale vor fi mult mai bine conectate;
- Elementele de avertizare vor fi mult mai responsabile;
- Urmele lăsate vor deveni din ce în ce mai mici.

Fiecare din aceste îmbunătățiri vor face posibilă înțelegerea diferențiată a lucrurilor. Trebuie să conștientizăm că proprietățile NCW oferă oportunitatea armonizării eficiente între abordarea asupra caracteristicilor câmpului de operații și a condițiilor de obținere a eficienței la cele mai înalte nivele.

Entitățile decizionale „intelligente" vor fi capabile să abordeze problemele într-un mod diferit față de acele entități mai puțin „intelligente". Procesul decizional nu se va mai concentra pe abordarea defensivă care presupunea adoptarea măsurilor de securitate împotriva incertitudinilor ci pe dimensiunea proactivă.

Partajarea cunoștințelor va determina delimitarea distinctă a capacităților adversarului. Aceasta presupune să acordăm mai multă atenție modelării câmpului de operații și mai puțină atenție la reacția și la schimbările bruște sau neașteptate.

Astfel planificarea va presupune mai multă economie de energie și resurse. C2 și execuția vor deveni un proces integrat în care eforturile vor fi canalizate pe monitorizarea implementării deciziilor și modificărilor în timp real.

Entitățile inteligente vor transforma abordarea privind funcția de comandă-control de la un proces **rigid** de planificare și decizie la un proces de **transmitere** a scopurilor și intențiilor și de orchestrare a sprijinului necesar executării deciziilor. Pe măsură ce se renunță la detalii viteza de comandă va crește. Mecanismul C2 va fi redus la nevoia de informație ceea ce va contribui la creșterea mobilității.

O mai bună **conectivitate** între actori și entitățile decizionale va genera creșterea capacității de reacție la modificările de situație. Mobilitatea se va extinde în condițiile în care entitățile responsabile cu procesul de avertizare vor avea mai multă putere de decizie.

Capacitatea de reacție la modificările de situație va avea implicații profunde pentru C2 și pentru activitatea de planificare. Planificarea va deveni un proces mult mai ușor cu cât mai mulți factori vor fi responsabili de acest lucru.

Capacitatea de optimizare a operațiilor va tinde să facă din planificare un proces continuu care se va îmbina, în anumite circumstanțe, cu procesul de executare.

La orice nivel dat, aceste schimbări vor modifica radical natura proceselor de comandă-control prin acordarea de responsabilități eșaloanelor inferioare. În ciuda creșterii ritmului de executare a operațiilor, entitățile decizionale de la cele mai înalte nivele vor beneficia de mai mult timp și resurse necesare monitorizării situației, identificării problemelor care apar și rezolvării cât mai rapide a acestora.

NCW oferă nu numai oportunitatea de rezolvare sincronizată a operațiilor ci și de examinare a proceselor de C2 fondate pe coordonarea orizontală, de sincronizare proprie a entităților implicate.

Aceasta adaugă o nouă dimensiune proceselor de comandă-control. Este recunoscut faptul că un anumit tip de comportament organizațional poate fi influențat sau chiar controlat fără probleme de sus în jos. NCW oferă alternativa obținerii rezultatelor dorite prin altă metodă. Comportamentul organizațional reprezintă o proprietate emergentă care derivă din:

- intențiile comandantului (interiorizate de actorii implicați);
- din gradul de cunoaștere a câmpului de operații;
- capacitatea entităților decizionale de a gestiona și diminua

constrângerile determinate de alocarea limitată a resurselor. Este dificil de supraestimat impactul pe care această nouă dimensiune a C2 îl va avea asupra viitorului mod de desfășurare a operațiilor.

Câmpul de operații al viitorului, din punctul de vedere al dimensiunii și naturii, va fi mult mai complex. Procesul de comandă-control se va confrunta cu această nouă dimensiune complexă.

Până nu demult se considera că, dacă dispunem de tehnologie avansată și de mecanisme organizaționale sofisticate, putem deveni stăpâni pe situație.

Se consideră că, dacă putem înțelege procesele de la bază putem manevra cu ușurință orice situație la orice nivel printr-o eforturi și analiză riguroasă. Iar dacă avem destul timp și energie intelectuală putem dezvolta un anumit nivel de înțelegere necesară operațiilor eficiente.

Azi mulți specialiști au ajuns să pună sub semnul întrebarii această viziune tradițională a problemelor complexe. Ei au semnalat că multe din procesele simple nu pot fi modelate adecvat cu toată tehnologia modernă și sofisticată de care se beneficiază.

Gestionarea sistemelor și situațiilor complexe este corelată inerent cu procesele de comandă-control. NCW oferă posibilitatea de a deveni stăpâni pe situație și de a depăși comportamentele aberante ale sistemului.

NCW oferă, de asemenea, posibilitatea de a compara și îmbina procesele decizionale ierarhice, caracteristice perioadei industriale, cu modelele descentralizate care acordă putere de decizie unităților mici.

Noua viziune asupra procesului C2 se bazează pe coroborarea acestor două tipuri de modele decizionale, utilizate fie separat, fie simultan, în funcție de tipul de misiune. Viitoarea arhitectură a procesului de comandă-control, modalitatea de îndeplinire a fiecărei misiuni, funcția și misiunea vor fi gestionate astfel încât să fie acoperit tot spectrul de probleme și comportamente.

Cu alte cuvinte, scopul procesului de comandă-control - acela de realizare a eficienței forțelor - va fi atins luând în calcul riscurile care trebuie aduse la nivelul de acceptabilitate, de la toate nivelele de comandă.

Există mai multe modalități de a lua în considerare riscurile. Astăzi se înregistrează amplificarea riscurilor neliniare care determină creșterea complexității câmpului de operații. Efectele amenințărilor neliniare se manifestă disproporționat în funcție de modificarea diferitelor variabile.

Dacă într-o organizație (sistem) predomină comportamentul liniar-determinist, o modificare minoră în cadrul structurii (input) va determina efecte minore (output). Într-un sistem neliniar în care predomină discontinuitatea, o modificare mică poate avea efecte majore (output) asupra structurii sistemului care se poate transforma ireversibil.

Putem translata această teorie asupra câmpului de operații care se va confrunta în viitor cu presiuni diferite de cele de până acum. Procesul tradițional de comandă-control urmărea să desfășoare lupta cu număr redus de victime umane. Abordarea actuală asupra C2 urmărește să diminueze erorile și să reducă gradul de vulnerabilitate la riscuri.

Dar, pentru era informațională nici această abordare nu mai este valabilă deoarece se bazează pe un număr redus de informații și pe importanța forțelor.

La momente diferite au fost adoptate abordări diferite care răspundeau cel mai bine condițiilor momentului istoric respectiv.

Astăzi, în condițiile creșterii galopante a ritmului schimbării, se urmărește reducerea riscurilor asociate amenințărilor neliniare precum și transformarea acestora în oportunități de exploatat în favoarea forțelor proprii, în vedere eficientizării operațiilor.

Viteza de comandă

În abordarea noastră asupra procesului de comandă-control (organizație, sistem) o măsură de bază constă în viteza de comandă, sau timpul necesar recunoașterii și înțelegerii situației, identificării sau evaluării alternativelor, selectării opțiunii celei mai optime și implementării prin ordin (comandă).

Dacă alternativa este corectă, planificarea va fi eficientă. Replanificarea este un proces consumator de timp și de resurse

ceea ce reduce eficiența operațiilor. Un prim pas în tot acest proces îl reprezintă înțelegerea corectă a problemei.

În operațiile tradiționale, cunoștințele sunt temporare deoarece totul se schimbă în ritm foarte rapid. Un motiv pentru care planificarea inițială nu are efectul scontat constă tocmai în această lipsă de informații cu valoare adăugată. Mai ales la nivelul eșaloanelor inferioare necunoașterea situației duce la eșuarea planificării inițiale și la întârzierea procesului decizional.

NCW duce în schimb la **creșterea vitezei de decizie și comandă.** Aceasta a fost ilustrată în timpul crizei din Taiwan, în 1995, când China a încercat să influențeze alegerile prin manifestări și amenințări zgomotoase.

Aceasta până în momentul intervenției americane cu două grupuri de armate. Pentru demonstrația noastră ceea ce este interesant este tocmai această modalitate diferită de exercitare a funcției de comandă-control.

Natura structurii comenzii la nivelul amiralității s-a modificat în momentul în care vice-amiralul Clemins, comandantul Flotei a 7-a a decis să reducă timpul destinat planificării de la zile la ore. S-au utilizat **e-mailul și tele-conferința** pentru a crea și menține la un înalt nivel gradul de cunoaștere comună a situației.

S-a pus foarte mare accent pe **partajarea** informațiilor în scopul eficientizării colaborării. Aceasta a accelerat procesul de sincronizare a operațiilor desfășurate de cele două grupuri militare americane din Taiwan.

La nivel tactic seria de experimente desfășurate de flota americană a demonstrat că puterea de luptă poate fi amplificată prin sincronizarea operațiilor, prin punerea în comun a informațiilor depre tabloul descriptiv al câmpului de operații.

La nivel operațional, Doctrina Întrunita pune accent pe dezvoltarea gradului de mobilitate a forțelor, menținerea și accelerarea ritmului operațiilor și angajarea prin surprindere a forțelor adversare în locurile și momentele oportune forțelor proprii.

S-a estimat și realizat calculul gradului de șoc, de impact asupra forțelor adversare și de producere a confuziei în scopul dezintegrării și anihilării adversarului.

TABLOUL OPERAȚIONAL COMUN
- cunoștințe partajate -

Un concept asociat îl reprezintă cel de ***Blocare strategică***.

Reprezintă activitatea de blocare a adversarului de a-și atinge obiectivele strategice. Chiar dacă ipoteza rămâne încă nedemonstrată, firul logicii ne conduce la ideea că blocarea strategică poate juca un rol-cheie acordând posibilitatea de încheiere rapidă a ostilităților.

Repetiția

O bună repetiție (simulare) poate avea efecte semnificative în ceea ce privește creșterea gradului de combativitate. Prin exploatarea infrastructurii informaționale tipică operațiilor de tip NCW actorii implicați au acces la informațiile comune, la instrumentele de planificare și simulare.

Acestea oferă posibilitatea executării repetate a operațiilor de simulare ceea ce duce la îmbunătățirea planurilor inițiale, la extinderea cunoașterii și, evident, la creșterea posibilității de obținere a succesului.

Extinderea cunoașterii

Actualele aplicații software (**AFMSS, PowerScene, TopScene**) permit actorilor din teatrul de operații să își dezvolte cunoașterea caracteristicilor câmpului.

De exemplu, un pilot poate simula misiunea de câteva ori pentru o mai bună cunoaștere a zonei de decolare, a rutei de intrare, a rutei de ieșire, a zonei de angajare.

Amenințările, cum ar fi stațiile de tip radar sau complexele cu rachete sol – aer (SAM) poate fi reprezentată tridimensional, permițând pilotului să planifice și să repete misiune pentru a diminua posibilitatea de a fi detectat de sistemele inamicului.

Aceasta conduce la creșterea posibilității de supraviețuire prin faptul că pilotul poate să își selecteze ruta de zbor astfel încât să nu fie descoperit de radare. Mai mult, simularea misiunii va

permite pilotului să crească posibilitatea de identificare și atingere a țintei. Sau la descoperirea erorilor de planificare sau de stabilire incorectă a coordonatelor țintei.

Fiecare din aceste exemple a fost testat în Operația din Bosnia (august-septembrie 1995) când au fost debarcate echipajele aeriene NATO.

Informațiile partajate asupra câmpului de operații au dus la creșterea preciziei și gradului de letalitate, la reducerea pagubelor colaterale și la pierderi minime.

Au fost atacate cu succes 97% din țintele vizate și distruse 80%. Țintele care constau în 338 de puncte vizate de lovire și destinate atacului din interiorul a 48 de locații au fost studiate și calculate pentru a se elimina pe cât posibil victimele din rândul populației civile. Pe parcursul întregii operații a fost doborât doar un singur avion,

Mirage 2000 al cărui echipaj a supraviețuit fiind repatriat. Totul a fost posibil datorită informațiilor oportune și corecte privind forțele adversare și dispunerea lor precum și despre mediul înconjurator.

Executarea comenzii

Am văzut că prin utilizarea noului concept NCW ni se oferă posibilitatea amplificării cunoașterii câmpului de operații, dezvoltării de noi abordări asupra procesului de comandă-control, de planificare și simulare eficientă.

În finalul acestei analize trebuie să vedem în ce mod toate acestea pot fi implemetate (executate). Entitățile implicate vor avea acces la informație și expertiză așa cum am explicat în paginile anterioare. NCW le permite să comunice cu celelalte entități aflate în câmpul de operații. Dacă transmiterea mesajelor se face corect, atunci gradul de cunoaștere se va extinde, oferind oportunitatea de a fi exploatată la maximum de eficiență.

Să presupunem că, pentru viitorul imediat, capacitățile fizice (sistemele de armament) rămân esențiale. Această presupunere nu poate fi rezonabilă deoarece dezvoltarea sistemelor de armament necesită timp pentru transport și desfășurare. Această

presupunere ne determină să minimizăm adevărata valoare a conceptului de NCW.

Dacă el nu va fi implementat cât mai curând, se comite o eroare de proporții. Cu alte cuvinte necesitatea este să vedem cum putem utiliza cel mai bine sistemele de armament folosind conceptele specifice NCW.

Eficiența desfășurării actorilor în câmpul de operații depinde de câteva caracteristici-cheie ale acestora:

- țintele pe care le pot ataca;
- expunerea la atacul adversarului (gradul de expunere la risc);
- viteza de comandă și rata atacului pe care îl pot susține;
- responsabilitatea unităților de sprijin;
- mobilitatea forțelor;
- letalitatea forțelor;
- extinderea gradului de sincronizare.

Adoptarea conceptului NCW ne oferă capacitatea de lărgire a atacului, de reducere a profilului riscului, de creștere a ritmului operațiilor și responsabilităților, de îmbunatatire a mobilității forțelor, de obținere a unui grad cât mai mare de letalitate.

Superioritatea Informațională, NCW și avantajul cunoștințelor (informațiile cu valoare adăugată)

Acest raport tratează un fenomen socio-cultural care a apărut în domeniul Apărării care a devenit o problemă comună, aceea că succesul unui război modern se realizează numai dacă este obținută Superioritatea Informațională. În rândurile care urmează se urmărește demontarea acestei afirmații. Argumentele pornesc de la lucrări de referință aparținând domeniului military cum sunt:

- Începe cu o scurtă descriere a contextului socio-cultural în care a apărut acest fenomen. Descrirea se face folosind concepte-cheie din lucrarea ***Joint Vision 2010*** și ***Strategia Politică Australiană.***
- Urmează apoi o secțiune dedicată Superiorității Informaționale și Superiorității Cunoaștințelor.

Succesul NCW presupune Superioritatea Cunoştintelor utilizând Superioritatea Informaţională.

• Se continuă apoi cu relaţia deosebită dintre superioritatea decizională şi războiul de manevră; superioritatea cunoştinţelor şi cunoştinţele despre război.

Succesul în războiul de manevră se obţine numai prin Superioritatea Cunoştinţelor.

• Se tratează apoi problema Superiorităţii Informaţionale şi superiorităţii cunoştinţelor în războiul de manevră. Lucrare de referinţă: ***Manevra decisivă.***

Succesul războiului de manevră presupune superioritatea cunoştinţelor utilizând superioritatea informaţională.

• În continuare se tratează natura avantajului Cunoştinţelor şi relaţionarea cu avantajul Deciziei şi avantajul informaţiilor.

Decizia presupune cunoştinţe utilizând informaţiile.

Raportul se încheie cu o discuţie pe temele tratate şi cu câteva recomandări privind evoluţia viitoare a fenomenelor discutate.

Superioritatea Informaţională, cunoaşterea şi Network centric Warfare

Martin Burke,

1. Contextul

Toate argumentele legate de NCW şi avantajul Cunoaşterii prezentate aici utilizează concepte care vor fi dezvoltate pe parcursul raportului.

2. Fundamente ştiinţifice

• **Joint Vision 2010** care reprezintă ***modelul conceptual pentru armata americană***. Se subliniază importanţa obţinerii

cunoștințelor privind câmpul de operații prin intermediul sistemelor de sisteme care utilizează sistemele tehnologice integrate.

„Ne trebuie Superioritatea Informațională: capacitatea de a colecta, procesa și disemina într-un flux continuu, neîntrerupt simultan cu exploatarea sau blocarea adversarului de a face același lucru."

„Baza acestui cadru de lucru o regăsim în îmbunătățirea funcțiilor de comandă-control și a activității de intelligence care pot asigura superioritatea informațională."

• **Strategia Politică a Australiei (ASP97)** stabilește direcțiile pentru apărarea secolului 21. Ea explică de ce în războiul viitorului victoria se va obține prin obținerea, pe cât este posibil, a tuturor informațiilor relevante despre adversar.

Se sublinia că avantajul Cunoașterii (exploatarea eficientă a tehnologiilor informaționale în scopul obținerii rezultatelor maxime cu minim de forțe), reprezintă cea mai înalta capacitate care trebuie dezvoltată prioritar.

Nici unul din cele două documente nu pun accentul pe Superioritatea Cunoștințelor. Acest termen este utilizat în raport ca desemnând **capacitatea de inducere în eroare a adversarului în scopul creări confuziei și adoptării deciziilor greșite.** De asemenea, nici unul din cele două documente nu pun accent pe factorul uman, purtător și transmițător de cunoștințe și informații. Ele pun accentul mai degrabă pe Superioritatea Informațională asupra adversarului decât pe producerea confuziei în rândurile acestuia.

Situația poate fi interpretată ca un fenomen socio-cultural în care predomină alți factori decât cei rationali. Acest raport nu urmărește nicidecum o analiză a fenomenului socio-cultural. Această problemă a fost tratatată în lucrarea ***Sisteme de gândire și NCW*** **(Burke, 2000).**

3. Obiective, abordare, structură

Raportul urmărește să aducă contraargumente ideii conform căreia „în războiul modern succesul poate fi asigurat prin Superioritate Informațională".

Demonstrația se va face pornind de la acele definiții și explicații din cele două lucrări descrise mai sus, **JV2010 și ASP97**.

4. Superioritatea Informațională, Superioritatea Cunoștințelor și NCW

În lucrarea **Network Centric Warfare (Alberts, Garstka et al., 1999)** s-a încercat demontarea ideii conform căreia „în războiul modern succesul poate fi asigurat prin Superioritate Informațională".

NCW este definit ca: ***superioritate informațională care duce la creșterea puterii combative prin senzorii din rețele, factori de decizie urmărind obținerea punerii în comun a cunoștințelor, creșterea vitezei de comandă și a sincronizării forțelor. În esență Network Centric Warfare translatează Superioritatea Informațională în putere de luptă prin eficientizarea legăturilor dintre entitățile din câmpul de operații. Puterea Network Centric Warfare este derivată din eficiența legăturilor din rețele sau punerea în rețele a entităților dispersate din punct de vedere geografic.***

Superioritatea Informațională este redefinită astfel: ***stare care este realizată atunci când avantajul competitiv este derivat din capacitatea de exploatare a poziției superioare din punct de vedere informațional.***

Această vedere revizuită este și ea eronată. Avantajul competitiv în NCW nu presupune în mod necesar o superioritate informațională în cazul în care un actor poate crea confuzie în rândurile adversarului fiind mai bine informat decât acesta.

Concluzie:

Succesul NCW presupune Superioritatea Cunoștințelor utilizând Superioritatea Informațională.

5. Superioritatea decizională și războiul de manevră; Superioritatea Cunoștințelor și Războiul Informațional.

În lucrarea ***Manevra decisivă* (1998)** acest concept este definit astfel: *conducerea sincronizată a operațiilor folosind toate*

mijioacele mobile și imobile din mediul respectiv în scopul atacării punctelor critice, vulnerabile ale adversarului puntru cucerirea punctului central și obținerea succesului maxim.

Superioritatea Decizională este definită astfel: ***Decizia luată într-un anumit ritm astfel încât forțele să fie capabile să utilizeze în mod superior cunoștințele atât pentru sucesul propriu cât și pentru a bloca accesul adversarului la astfel de informații despre forțele proprii.***

Relația dintre superioritatea decizională și războiul de manevră poate fi sintetizată astfel:

- Războiul de manevră este războiul modern;
- Războiul de manevră conține războiul Informațional (al cunoștințelor);
- Succesul în războiul de manevră presupune Superioritatea Decizională;
- Succesul în Războiul Informațional presupune Superioritatea Cunoștințelor;
- Superioritatea Decizională presupune Superioritatea Cunoștințelor.

Concluzie:

Succesul în războiul de manevră se obține numai prin Superioritatea Cunoștințelor.

6. Superioritatea Informațională, Superioritatea cunoștințelor și războiul de manevră.

În aceeași lucrare, *Manevra decisivă* (1998), se clarifică relația dintre Superioritatea Informațională și Superioritatea Decizională: ***Conflictul reprezintă un proces dinamic în care rezultatele acțiunilor planificate nu pot fi complet predictibile. Chiar și în cazul celui mai bun plan nu putem ieși complet teferi din conflictul cu un adversar. Pentru a fi eficientă manevra decisivă trebuie să se bazeze pe monitorizarea continuă a situației pentru a fi capabili să reacționăm mult mai repede decât adversarul. Aceasta se obține prin Superioritatea Decizională, dezvoltată***

printr-un management informațional superior și asigurat de o stare robustă de securitate.

Aspectele relevante sunt următoarele:

• Succesul războiului de manevră presupune Superioritate Decizională;

• Succesul războiului de manevră utilizează Superioritatea Informațională.

Concluzie:

Succesul războiului de manevră presupune superioritatea cunoștințelor utilizând superioritatea informațională.

7. Decizia, Cunoștințele și Informațiile

În orice conflict unul dintre adversari beneficiază de superioritate. În mod particular, în războiul de manevră:

• Avantajul decizional există doar la cel care beneficiază de superioritate asupra celuilalt.

• În Războiul Cunoștințelor avantajul cunoștințelor există doar la cel care beneficiază de Superioritatea Cunoștințelor asupra celuilalt.

• În războiul Informațional avantajul informațional există la cel care beneficiază de superioritate Informațională asupra celuilalt.

Avantajul decizional presupune avantajul Cunoștințelor utilizând avantajul Informațiilor.

Această aserțiune poate fi întărită printr-un citat din lucrarea *Manevră decisivă:*

Pentru ca Inovația să aibă efectele dorite trebuie să se bazeze atât pe cunoașterea comprehensivă a punctelor tari, punctelor slabe și intențiile ale adversarului cât și pe cele proprii. Desfășurarea oricărei acțiuni trebuie să se bazeze pe cunoașterea detaliată a mediului strategic și tactic pentru a diminua posibilitatea apariției efectelor nedorite.

Mai departe se subliniază faptul că există diferențe profunde între natura corpului cunoștințelor și forțele militare. O trăsătură necesară obținerii și menținerii avantajului cunoștințelor va fi înțelegerea potențialului inamicului și a felului în care acesta este exploatat.

De asemenea, trebuie să înțelegem că superioritatea cunoștințelor asupra unui inamic nu înseamna superioritate și asupra altui inamic. Acesta este un concept relativ.

După cum trebuie să înțelegem că este totodată și un concept dinamic, care suportă schimbări rapide în urma interacțiunilor sistemului cu presiuni noi.

8. Discuții și concluzii

Raportul a supus observației auditoriului apariția unui nou fenomen socio-cultural în comunitatea Apărării care pornește de la ideea că „**în războiul modern succesul poate fi asigurat prin Superioritate Informațională**". Pe tot parcursul raportului au fost prezentate argumente în scopul demontării acestei aserțiuni care tinde să fie generalizată.

Concluziile la care s-a ajuns în urma discuțiilor sunt următoarele:

- În NCW succesul presupune Superioritatea Cunoștințelor utilizând Superioritatea Informațională;
- Succesul războiului de manevră presupune superioritatea cunoștințelor utilizând superioritatea informațională;
- Avantajul decizional presupune Avantajul Cunoștințelor utilizând Avantajul Informațiilor.

Totuși trebuie să amintim că acest raționament nu este complet riguros dar este plauzibil având în vedere că se bazează pe două surse doctrinare: **JV2010 și ASP97**. Apărarea militară nu trebuie privită ca un fenomen static și stabil care poate fi înțeles sau perfect realizabil, ci ca un fenomen dinamic, volatil și eluziv. De aceea sunt necesare metode noi, diferite de cele adoptate până acum pentru a analiza și gestiona acest fenomen. Este neceasară învățarea și aplicarea acestor metode specifice războiului viitorului.

Războiul Informațional și Războiul Cunoștințelor

Această anexă prezintă **două fragmente** de referință din lucrarea lui **Philippe Baumard,**

De la Războiul Informațional la Războiul Cunoștințelor **(1996).**

„Există iluzia că dezvoltarea unei structuri informaționale este o condiție necesară și suficientă pentru a dobândi infrastructura națională a cunoștințelor. Din contră, o astfel de politică se dovedește contraproductivă. Ea va conduce la separarea corpului cunoștințelor de la cele mai înalte nivele care se va rupe de realitățile sociale cotidiene și, în cele din urmă la crearea unei nișe între oamenii care acționează, învață, vorbesc și oameni care au acționat, au învățat, au vorbit."

*

„Wilenski spunea că **„informația a fost o sursă de putere iar azi a devenit o sursă de confuzie"**. În fiecare sferă a vieții moderne s-a produs o suprasaturare cu informație, care a dus de cele mai multe ori la pierderea sau integrarea deficientă în sistem. Rădăcinile acestei probleme sunt următoarele:

(a) confuzia persistentă dintre informații și cunoștințe,

(b) concentrarea sistemului educațional actual pe acumularea de cunoștințe de bază vs. îmbunătățirea diversității și flexibilității modelelor de gândire,

(c) eșecul introducerii în entitățile organizaționale a ideilor novatoare. Managerii sunt conștienți că fenomenul adaptabilității este o asigurare în găsirea celor mai eficiente soluții pentru rezolvarea problemelor organizaționale. Cu toate că există o percepție destul de consistentă asupra cunoașterii, predomină distincția netă între conceptul de „organizație" și cel de „cunoștințe/cunoaștere".

Specialiștii în teoria organizațiilor au propus o serie de soluții alternative originale care pun accentul pe socializare și participarea colectivă la construcția organizațională și la generarea cunoștințelor"

Kasparov vs. Kasparov

Această anexă cuprinde un studiu de caz care să ilustreze dependența de informație în timpul unui conflict. Kasparov este un jucător de șah fanatic. A studiat multe cărți de șah și a analizat multe partide istorice.

Fiul său Gary a fost învățat de mama sa să joace șah la o vârstă foarte timpurie. La 4 ani a bătut-o la șah pe mama sa pentru prima dată.

Kasparov tatăl, evident, avea mai multă experiență șahistică decât fiul său. Fiul nu a avut acces la informația la care nici mama nu a avut acces, în ciuda acestui dezavantaj talentul său precoce i-a permis să își dezvolte cunoștințele despre modalitățile de joc, etc. Astfel a întrecut-o pe mama sa.

Acest exemplu ne demonstrează că superioritatea informațională nu este de ajuns pentru a câștiga într-un conflict de cunoștințe.

Învatamintele acestei istorioare sunt:

- Ambii jucători aveau informații complete și identice;
- Kasparov tatăl avea mai multe informatii decât fiul său;
- Gary Kasparov nu a dispus de informația relevantă de care nu dispunea nici mama sa.

Rezultă că superioritatea informațională nu este necesară pentru superioritatea cunoștințelor. Cazul ne demonstrează că în anumite circumstanțe abilitatea de a învăța și de a aplica aceste cunoștințe este mult mai importantă decât accesul la o multitudine de informații relevante. Aici există mai mulți factori explicativi:

- Informația codificată din ADN pe care mama a partajat-o cu fiul;
- Informațiile din creierul jucătorilor rezultate în urma observării jocului;
- Informațiile din cărțile de șah pe care Kasparov tatăl le-a citit și le-a interpretat;
- Informațiile transmise de la mamă la fiu pe parcursul învatarii și antrenării.

Cele 7 "păcate" ale NCW

Th. Barnett

Cei mai mulți dintre noi au citit articolul **vice-amiralului Art Cebrowski** din 1998 despre NCW și au putut vedea viziunea oarecum îndrazneata care era prezentată acolo. Pornind de la citatul lui Lidell-Hart „mai greu decât pătrunderea unei idei noi în armată este renunțarea la ideea învechită", Cebrowski și coautorul A. Gartska aruncă mănușa spre provocarea tuturor celor care le-ar putea dovedi că nu au dreptate absolută.

Autorul acestui articol urmărește să identifice și să comenteze unele neajunsuri ale NCW, după cum le-a numit „păcate, dar, atenție, nu păcate de moarte".

PATIMA

NCW tânjește după un adversar cu putere tehnologică. Este îndoielnic că, din această perspectivă, SUA s-ar putea confrunta cu un adversar pe măsură. SUA cheltuiesc pe tehnologie informațională mai mult decât ar cheltui două țări cu întreaga armată.

În timp ce aliații SUA se străduiesc să țină pasul cu americanii ne putem întreba în ce moment aceștia vor fi la fel de pregătiți din acest punct de vedere? Într-o lume în care națiunile cheltuiesc în medie 5 miliarde de dolari pentru Apărare, NCW reprezintă o cărare bătută doar de americani.

De aceea nici măcar aliații cei mai de seamă ai americanilor nu pot să țină pasul cu această cursă a „comunicării".

În continuare autorul ne vorbește despre manifestarea efectului **QWERTY***.

Acesta este clar monopolul americanilor, celelalte fiind doar simple copii mai mult sau mai puțin performante ale tehnologiei americane.

Să ne amintim momentul când Iranul a primit tehnologie pentru rachete de la Coreea de Nord. Aceasta reprezinta o copie

* De la computer, simbolurile primelor taste

pentru rachete de la Coreea de Nord. Aceasta reprezinta o copie

săracă a tehnologiei chinezești, o copie și mai săracă a tehnologiei sovietice, și o copie și mai săracă a tehnologiei naziste**.

Iată de ce proliferarea rămâne mai lentă decât sugerează cei mai mulți experți în legătură cu NCW.

Dacă țările competitoare se apropie cât de cât de performanțele tehnologice americane, țările mici, inamice ale SUA, care își revendică drepturile evident nu pot fi considerate inamice din perspectiva NCW.

În aceste condiții SUA ar trebui să își tempereze patima după adversari demni din perspectiva NCW.

NEPĂSAREA

Militarii americani se adaptează foarte lent la NCW în lumea "**MOOTW**" (operațiile militare altele decât războiul). Acestui tip de operații trebuie să le facă față militarii americani azi.

De aceea se pune problema cum s-ar putea aplica NCW aici? Soldații să comunice între ei prin cabluri? Sau să comunice cu lumea exterioară?

Aceasta nu este o întrebare ezoterică pentru forțele navale deoarece va veni un moment când rețeaua informațională va deveni crucială pentru marina americană în momentele de criză mai ales când predomină confuzia și haosul. De aceea NCW trebuie să reprezinte o cale spre rezoluție și nu spre conflict. Forțele navale trebuie să reprezinte un „nod" conector, nu un nod distructiv.

Dacă va fi folosit corect NCW va permite militarilor americani să intervină pentru rezolvarea oricărei situații de criză și să instaleze o „**umbrelă informațională**" care să facă reclamă transparenței acțiunilor întreprinse.

ZGÂRCENIA

NCW promovează principiul „mult și ieftin" în timp ce armata merge pe „puțin și scump". Mulți experți susțin, și pe drept cuvânt, că NCW nu aduce nimic nou față de marină.

** Nimic mai fals, și tehnologia de rachete americană are ca sursă tehnologia de rachete nazistă (nota S.E.)

Marina americană reprezintă un mediu interconectat. În toate serviciile importante din acest departament avem de-a face cu conectare de tip NCW. Nu este nici un secret pentru nimeni că Marina a sacrificat un număr important de vase în favoarea achizițiilor tehnologice.

Ceea ce ne face să estimăm că Marina va sărăci în viitoarea eră a NCW unde contează mobilitatea și flexibilitatea. Pentru că șansele de confruntare cu inamici aflați în paradigma „puțin și ieftin" sunt foarte mari. De aceea paradigma americană „mult și scump" nu va mai fi funcțională.

MÂNDRIA

Strategiile de blocare specifice NCW vor duce la resuscitarea vechiului mit al bombardamentului strategic.

Până în 1921 (Giulio Douhet, *Comanda aerului)* se credea că o lovitură aplicată în centrul de greutate a inamicului conduce la o victorie rapidă fără victime.

Această paradigmă persistă și azi în viziunea teore-ticienilor NCW prin conceptul de „Blocare strategică". Chiar dacă oponenții NCW admit sau nu, cele două strategii au în comun ideea falsă că pedeapsa înseamnă control. Distrugând tehnologia informațională a inamicului, înseamnă că îl anihilăm?

Nu. De ce?

În primul rând pentru ca RI desfășurat de o țară reprezintă terorism internațional desfășurat de o altă țară. Dacă o putere ostilă ar încerca să deformeze scopurile noastre am fi acuzați de tot felul de crime de război.

Pagubele colaterale asociate decapitării tehnologiei informaționale sunt prea complexe pentru a fi controlate de la distanță.

În al doilea rând structurile responsabile cu evaluarea pagubelor produse de bombardamente sunt azi capabile să măsoare și efectele în masă ale NCW. Unii presupun că micșorarea gradului de tehnologizare informațională a societăților mici determină creșterea abilității americane de a înțelege impactul războiului informațional.

În al treilea rând, în timp ce salută această teorie complexă,

cel care promovează conceptul de NCW renunță la tot ceea ce înseamna blocare strategică.

În al patrulea rând NCW este vinovat de «imagine în oglindă": noi teoretizăm despre vulnerabilitățile tehnologiei noastre informaționale și presupunem, totodată că și alții fac același lucru.

FURIA

Presupunerile privind creșterea vitezei de comandă sunt generate de faptul că date și informații ne parvin cu viteză foarte mare. Acest cerc virtuos se poate transforma într-unul vicios dacă entitățile decizionale vor deveni sclave ale computerelor lor.

Rapiditatea cu care pot circula deciziile greșite, iată adevăratul pericol. Și mai îngrijoratoare sunt presupunerile privind intruziunea în mecanismul decizional al inamicului. Aceasta a devenit un scop cu toate că ar trebui să ne centrăm pe ceea ce trebuie să facem în momentul în care pătrundem acolo.

Vorbim mereu despre potențialul inamicului cu tehnologie informațională mai puțin dezvoltată, ceea ce face ca percepția deformată să fie uriașă.

INVIDIA

NCW râvnește spre sincronizarea cu lumea comercială a afacerilor. Nici o armată din lume nu este mai armonizată decât cea americană.

În nici o armată nu se urmărește scopul descentralizării deciziei ca în aceasta. Deci dacă vreo armată se va adapta la NCW prin realizarea principiului sincronizării, aceasta va fi cea americană. Scopul auto-sincronizării este acela că tehnologia informațională va facilita o transmitere extrem de rapidă a informației permițând comandanților să exploateze la maximum viteza de comandă. Invidia NCW față de lumea afacerilor din perspectiva sincronizării cu piața este o atitudine pe care o putem înțelege.

Aceasta deoarece operațiile militare sunt poate faptele cele mai complexe din lume. Dar această invidie este prost plasată. Sunt create guverne care să rezolve problemele spinoase ale societății pe care credem că firmele particulare nu le pot gestiona

sub motivația că scopul lor ultim este acela de a obține profit. Și, printre aceste probleme spinoase sunt și cele militare.

LĂCOMIA

Termenul „tablou comun al câmpului de operații" din viziunea teoreticienilor NCW desemnează faptul că toți actorii din câmpul de operații trebuie să îmbrățișeze același model mintal. Nu ne îndoim că numai prin intermediul prezentărilor multi-media se vor putea pune în comun informațiile despre realitățile câmpului de luptă.

Noutatea este reprezentată de capacitatea rapidă de inundare cu informații. În cazul în care acestea sunt eronate percepția eronată se poate generaliza iar deciziile adoptate vor fi evident greșite.

Ambiția NCW devine cu atât mai îngrijorătoare cu cât există fenomenul de filtrare la transmiterea informațiilor de la un nivel la altul de comandă. NCW promite să netezească ierarhiile, dar natura complexă și gravă a operațiilor militare poate împinge mai mulți comandanți la adoptarea unor decizii fanteziste.

Infuzia tehnologiilor informaționale în organizațiile ierarhizate reduce asimetriile tradiționale conform cărora doar entitățile din vârful piramidei beneficiau de informații complete. Din această perspectivă conceptul de „tablou comun al câmpului de operații" este o încercare de a limita prerogativele și tendințele exclusiviste ale înalților comandanți militari.

Tentația lăcomiei față de informații va exista întotdeauna la NCW.

CONCLUZIE

Aici nu s-a încercat nici să se discrediteze conceptul de NCW nici negarea sa. Trecerea în viitor a structurilor Apărării la paradigma NCW va fi inevitabilă.

Viitorul este al **RĂZBOIULUI în REȚEA.**

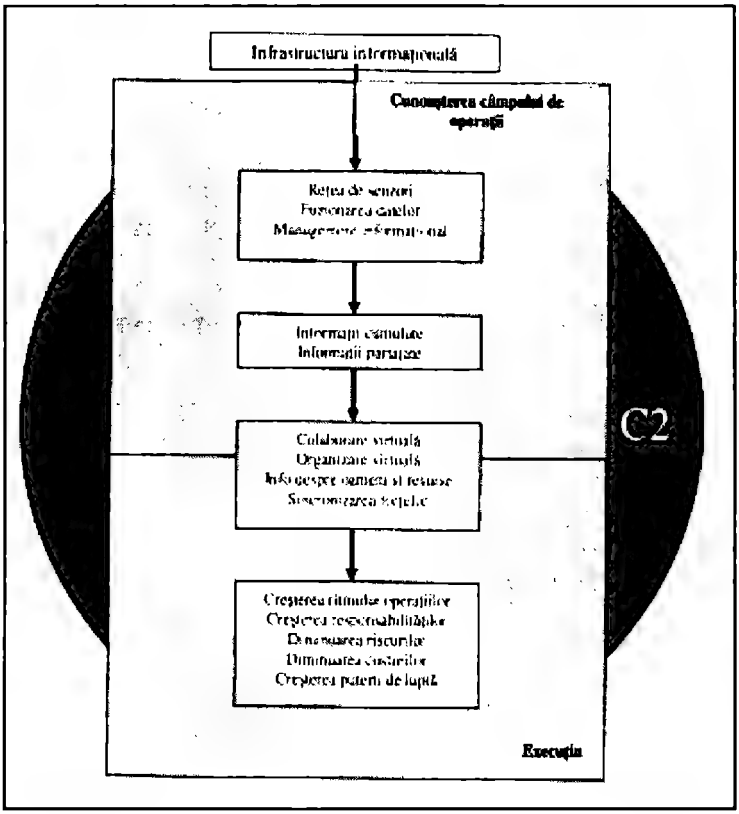


Figura 1 – **Infrastructura informațională**

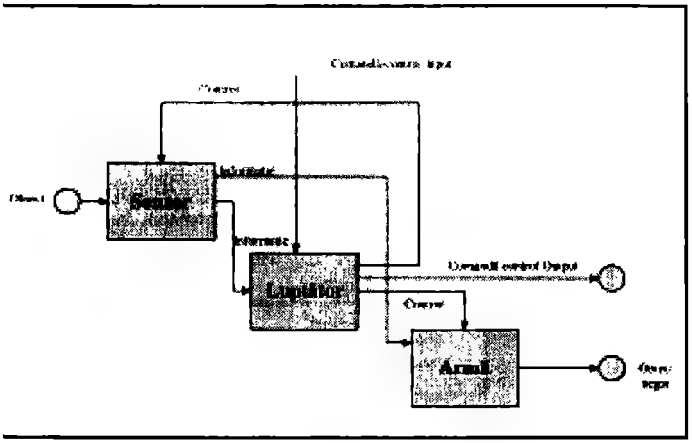


Figura 2 – **Componentele funcţionale ale angajării unui luptător comandând o „forţă“ în teren**

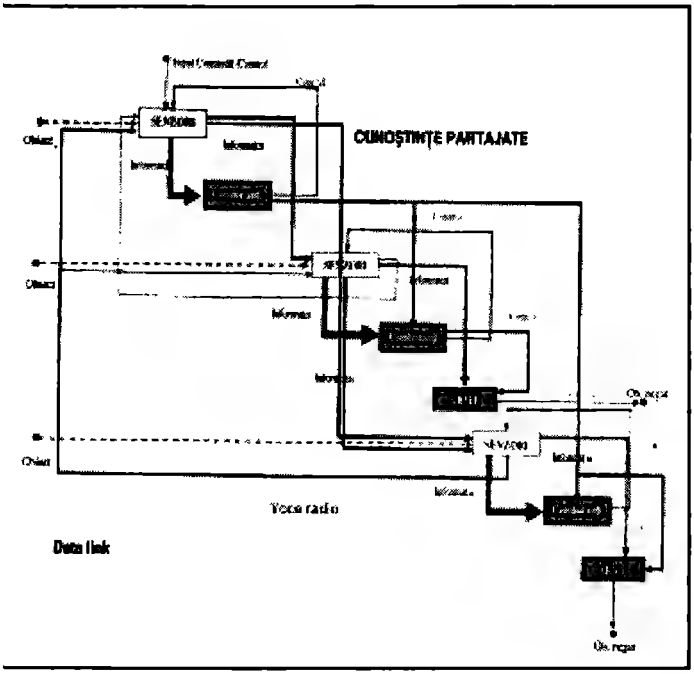


Figura 3 – **Nivele de cunoaştere ale cunoştinţelor partajate**

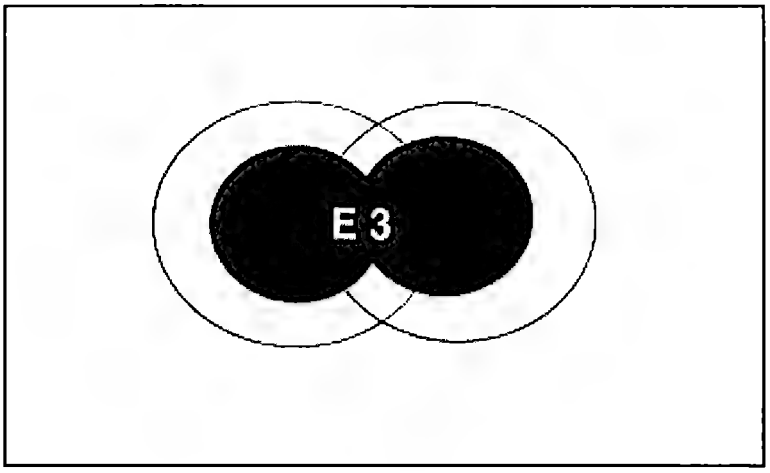


Figura 4 – **Platform Centric Engagement Envelope**

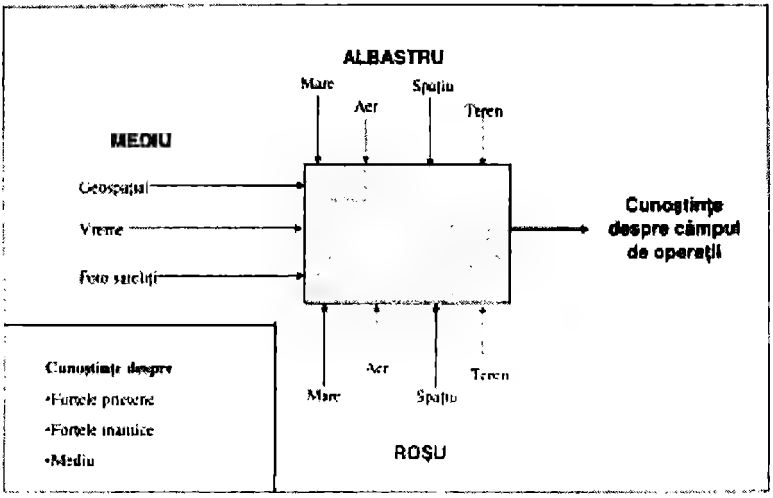


Figura 5 – **Cunoașterea cîmpului de luptă**

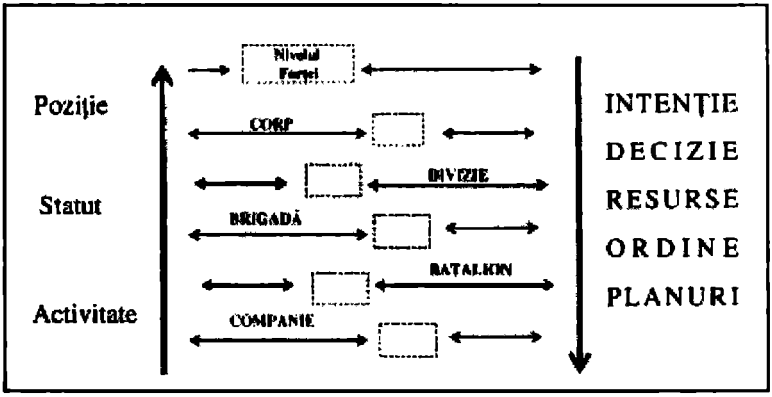


Figura 6 – **Partajarea informaţiilor pe eşaloane şi ierarhii**

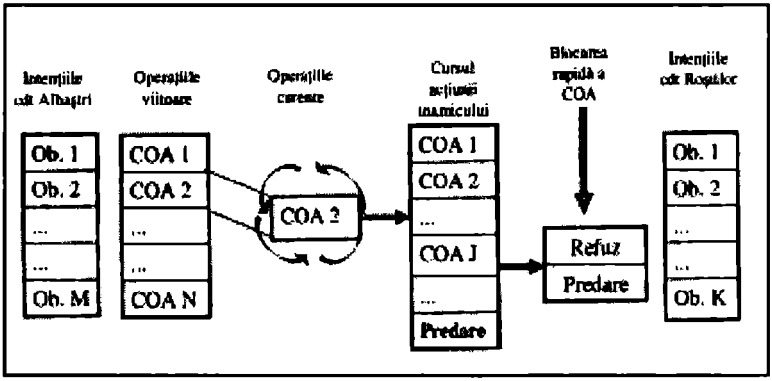


Figura 7 – **Conceptul de blocare strategică**

ANEXA 2

1. RĂZBOIUL INFORMAȚIILOR A DEVENIT DEJA O REALITATE A CÂMPULUI DE LUPTĂ MODERN

Evoluția tehnico-științifică contemporană extrem de spectaculoasă, se răsfrânge într-o măsură pregnantă atât asupra evoluției societății, cât și asupra dezvoltării organismului militar sub toate aspectele.

În câmpul de luptă modern, influența informațiilor devine hotărâtoare, cu însemnate repercursiuni asupra eficacității armamentului și moralului luptătorilor și, în consecință asupra deznodământului luptei. În societatea informațională, în contextul creșterii explozive a utilizării informaticii, comunicațiilor și mijioacelor de luptă cibernetizate, informația devine **obiectivul, mijiocul și procedura** unei noi forme de război - **războiul informațiilor.**

Pentru acest tip de război nu sunt încă **definiții** oficiale. O definiție acceptată de mai mulți specialiști a fost cea formulată de dr. John Alger de la Universitatea „George Washington" ca reprezentând: „acțiunile întreprinse pentru a asigura superioritatea informațională prin afectarea informațiilor, proceselor de prelucrare și a sistemelor informatice ale inamicului concomitent cu apărarea celor proprii.

O altă definiție a fost emisă de ministrul apărării al S.U.A.: „acțiunile întreprinse pentru asigurarea superiorității informaționale în sprijinul strategiei militare naționale prin afectarea informațiilor și sistemelor informaționale ale adversarului, concomitent cu apărarea și utilizarea în siguranță a sistemelor informaționale proprii".

După aprecierea majorității specialiștilor care au abordat războiul informațional, acesta ar viza cele **două componente** de bază (hardware și software) utilizate în:

- sistemele de comunicații;

- sistemele de calculatoare (rețele calculatoare, poștă electronică, etc.);

- sistemele de conducere și dirijare a tehnicii de luptă și armamentului;

- sistemele de război electronic (în general de bruiaj electronic);

- sistemele de război psihologic (în special dezinformarea).

Războiul informațional **poate fi:**

- de apărare (cuprinzând măsurile de protecție a sistemelor informaționale proprii);

- ofensiv (cuprinzând acțiunile de neutralizare a sistemelor informaționale ale adversarilor);

Războiul informațional **vizează:**

- controlul deciziilor și al modului de elaborare al acestora;

- paralizarea funcționărilor structurilor organizatorice și a relațiilor dintre acestea ;

- influențarca proceselor decizionale;

- structurile decizionale ale domeniului politic, economic, social și militar" ;

- blocarea fluxului informațional dintre factorii politici de conducere și organismul militar, dintre structurile politice și cele administrative, dintre structurile civile și cele militare, dintre conducere și luptătorul (executantul) propriu-zis;

- controlul general sau parțial asupra mass-media pentru denaturarea realității, și micșorarea oportunității informării, generarea confuziei și a neîncrederii în structurile politico-militare, în comandanți;

- crearea unei false atmosfere de neliniște ori de prea mare încredere;

- manipularea informațională a comandanților, populației și a luptătorilor;

- deturnarea sau anihilarea funcționării armelor inteligente și a sistemelor de conducere ale acestora"

- generarea și gestionarea crizelor informaționale.

Eficacitatea acțiunilor de luptă informațională este cu atât

mai mare eu cât este mai intensă, iar mijioacele de securitate ale adversarului sunt mai puțin performante.

Războiul informațiilor se **poartă** în toate mediile de ducere a războiului energetic și este dublat de un război electronic generalizat, astfel încât nimic nu începe, nu se desfășoară si nu se termină fără informații și contrainformații, fără prelucrări, procesări și transmiteri. Războiul informațiilor se poartă atât la vedere, cât și, mai ales în ascuns, cu mijloace și sisteme soffsticate, cu acțiune imediată sau cu efecte întârziate.

Perioadele cele mai acute ale războiului informațional sunt cele de criză în care abundă situațiile haotice, se diminuează capacitățile de orientare, se micșorează libertatea de acțiune, se mărește responsabilitatea deciziilor și se amplifică sentimentul de nesiguranță. De fapt, situațiile de criză constituie, pentru sistemele informaționale, adevăratele situații de test, în care tot ceea ce reprezintă neutilitate se accentuează, iar ceea ce înseamnă slăbiciune poate deveni catastrofală.

Forțele care poartă acest război:

- efectivele de luptă electronică specializate, care dispun de mijloace și posibilități deosebite, ce pot acționa direct în câmpul de luptă, precum și în mediile complementare;

- forțele de cercetare -diversiune, dotate cu mijloace mobile rapide și electronice performante de ultimă generație;

- sistemele de armament care includ și o componentă electronică (arme inteligente);

- „teroriștii informaționali", organizați sau pe cont propriu (izolați);

- spioni în slujba unor state sau organizații internaționale (structuri de informații ofensive);

- „hacker-ii" (spărgătorii de coduri și sisteme de securitate informațională de acțiune pe cont propriu, pentru plăcerea de a „demola" barierele oficiale și de a-și încerca forțele, dar care pot fi manipulați și utilizați, fără știința lor, de tot felul de organizații teroriste) ;

- „curioșii", utilizatori de sisteme și mijioace informatice conectați la sistemele interne sau internaționale și care iscodesc,

compară, analizează; schimbă și actualizează de dragul surprizei; aceștia deși în aparență inofensivi pot produce efecte considerabile, chiar catastrofale, dar pot fi și manipulați; ,

- Amatorii de senzații tari neinstruiți, neavizați, care, jucându-se cu calculatorul pot produce necazuri mari;

- sisteme inteligente, special destinate acestui scop și virușimarea nenorocire a epocii informaționale".

Nici unul din aceste atacuri nu trebuie subevaluat, fiecare fiind susceptibil de a produce pagube imense sau catastrofale economice, politice ori militare.

Multe din aceste activități sunt calificate de către specialiști drept crimă împotriva umanității.

În urma concluziilor desprinse din acțiunile de război informațional și din studiile întreprinse, armata americană a elaborât o nouă concepție de contracarare a efectelor războiului electronic sintetizată în câteva direcții de acțiune (10):

- asigurarea luptătorului cu sisteme specifice câmpului de luptă modern;

- optimizarea mijloacelor privind tehnologia informațională;

- implementarea securității informaționale la toate nivelele (acoperire prin criptare și alte metode);

- asigurarea supremației electromagnetice și utilizarea modului / TEMPEST-*

- utilizarea modelării și simulării în pregătire etc.

Principiile informațiilor

a) Suficiență informativă - principiul similar cu cel al suficienței de resurse energetice, financiare, etc.) are în vedere satisfacerea, în condiții de oportunitate a necesarului de informații atât pentru conducerea acțiunilor de luptă (în folosul statelor majore), cât și pentru executarea misiunilor de către sistemele de armament sau chiar de luptători individuali.

Suficiența informației reprezintă un principiu de echilibru stabilit în funcție de riscul operativ asumat și costul posibil dc suportat și determinat de :

- cantitatea și distribuția pe domenii a informației;

- capacitatea de procesare, prelucrare tactic-operativă și de transmitere a informației;

- ritmul actualizărilor și schimbărilor pe care le generează sau împiedică schimbul de date.

Între suficient și optim există o relație dinamică, fiind o valoare în jurul căreia oscilează suficientul.

Pericolele ignorării principiului suficienței informației sunt :

- subevaluarea - care determina lipsa de informații și deci o decizie insuficient documentată și susținută informativ;

- supraevaluarea - deci o cantitate mai mare a informațiilor decât cea necesară ceea ce duce la suprasaturarea informativă, îngreunarea selecției informațiilor utile, întârziere în procesare și transmitere, care afectează operativitatea în elaborarea variantelor și soluțiilor optime și, deci, întârzierea elaborării și aplicării hotărârii.

b) Proporționalitatea distribuției - principiul similar cu cel al structurii proporționale a forțelor necesare ducerii războiului și are în vedere distribuția, în funcție de necesități și zone de interes ierarhizat, a fluxului de informații pe problematicile conducerii, execuției și pe capacitatea de procesare și transmitere.

Acest principiu este suficient atunci când pentru fiecare domeniu în parte sau misiune se asigură o suficiență informativă, fără goluri mari sau vârfuri însemnate de informare.

Proporționalitatea distribuției informațiilor este rezultatul unei activități profesionale deosebite și trebuie satisfacută de dinamica acțiunilor de luptă, atât pe timpul elaborării hotărârii cât și pe timpul executant misiunilor, având în vedere că realitățile informative se schimbă foarte des, schimbarea nu este liniară, fiind greu de prevăzut și contracarat.

c) Oportunitatea informării - principiul cel mai invocat de analiștii militari, ce derivă din Oportunitatea hotărârilor și a operațiilor și are în vedere culegerea de informații în timp operativ -real, cât și procesarea și transmiterea acestora la mediile cu necesități de informare.

Oportunitatea informației are deci două componente (caracteristici):

- caracteristica temporal- dinamică;

- componenta dependentă de cantitatea de informații necesare de calitatea și credibilitatea acestora, de capacitatea de procesare și transmitere.

d) Credibilitatea informațiilor - cel mai vechi principiu, care pune în raport cantitatea de informații cu gradul de adevăr conținut.

Complexitatea principiului derivă din dimensionalitatea sa, care se referă la:

– credibilitatea surselor de informații interceptate;

– abilitatea și profesionalismul celor care interceptează sursele;

– siguranța transportului informațiilor (ne alterabile în timp);

– capacitatea de prelucrare și desprindere a adevărului;

– discernământul celor informați.

Experiența demonstrează că, nici după foarte mult timp, credibilitatea unei informații nu poate fi determinată și garantată.

e) Accesibilitatea informațiilor - este principiul cu valențe deosebite, astăzi în epoca informatizării și războiului cibernetic, însemnând capacitatea informațiilor de a se exprima direct și fără dubii prin semantica și modul lor de reprezentare.

Informația cea mai accesibilă este informația cu semantica definită, explicit, fără ambiguități, într-un limbaj adecvat destinatarului sau utilizatorului cu un anumit nivel de pregătire și grad de inteligență.

2. CARACTERISTICI ALE DINAMICII RESURSELOR INFORMAȚIONALE

- sporirea considerabilă a volumului informațiilor necesare elaborant hotărârii și ducerii acțiunilor de luptă (de 4-10 ori față de volumul informațiilor vehiculate în cel de al doilea război mondial);

- creșterea posibilităților de informare, prin diferite mijioace de culegere (interceptare radio, radiații electromagnetice, rețele, calculatoare, poștă electronică, etc.);

- sporirea necesităților și posibilităților de procesare și de sinteză logică, atât în sfera conducerii cât și în cea a execuției;

- influența fastă a procesării informațiilor asupra eficacității sistemelor de armament dar și cea nefastă a informațiilor de disimulare a virușilor calculatoarelor asupra proceselor de execuție specializate;

- creșterea explozivă a cantității de informații necesare luptătorului pentru a face față solicitărilor și vitregiilor câmpului de luptă modern;

- raportul de 9-13 la 1 între acțiunile de război informațional și cele de lovire efectivă;

- apariția, integrarea și utilizarea armelor de luptă inteligentă (roboți militari);

- apariția și perfecționarea structurilor specializate de securitate a informațiilor;

- legătura indisolubilă dintre moral și informare, dintre angajare și cunoaștere, dintre acțiunea profesionistă și realitatea câmpului de luptă;

- caracterul cibernetic al acțiunilor de luptă și apropierea informațională și tehnologică dintre conducere și execuție.

Structurile de informații militare este necesar să-și reconsidere unele elemente din Planul de căutare a informațiilor. Mă refer la faptul că ele urmează să-și pregătească componenta contra-informativă la asemenea parametri încât să fie capabili să facă față terorismului informațional. Aceasta reprezintă de fapt o utilizare abuzivă a sistemelor informative digitale, rețelelor sau altor componente pentru un rezultat final care sprijină sau facilitează o acțiune sau campanie teroristă. În momentul când infrastructura informațională va fi încheiată în armata noastră, ne putem aștepta oricând la acțiuni de acest gen.

Considerând că deocamdată, armata română se găsește încă departe de riscurile unor asemenea amenințări plecând în special de la premisa inexistenței unei infrastructuri generale adecvate, dar asemenea amenințări pot ajuta mult la pregătirea unor măsuri de protecție pentru cazul în care vom fi în măsură și vom avea ceva de apărat în acest domeniu.

3. OPERAȚIILE INFORMAȚIONALE

„În secolul XXI, operațiile se vor baza foarte mult pe cunoașterea rezultată din date și informații relevante culese, prelucrate, analizate și difuzate printr-un sistem global complex de sisteme. Acest cadru evolutiv de informare militară va schimba fundamental modul de desfășurare a operațiilor de către trupele de uscat în timp de pace și în conflicte... Trupele de uscat vor integra operațiile informaționale în fiecare aspect al concepției Trupele de Uscat XXI.

Folosind avantajele operațiilor informaționale, comandanții trebuie să fie conștienți că bizuirea trupelor de uscat pe tehnologiile de informare creează noi vulnerabilități și cursuri de acțiune asimetrice, avantajoase pentru inamic. Conceptul superiorității informative se bazează pe disponibilitatea de informație. De aceea, informațiile și sistemele de informare (INFOSYS) trebuie protejate. Operațiile informaționale se desfășoară într-un „cadru național total care adaptează mijloacele la obținerea superiorității militare (ca și a celei diplomatice și economice) asupra adversarului pe baza cunoașterii...„. Aceste concepte privind operațiile informaționale duc spre noi modalități de a gândi războiul, spre responsabilități noi și chiar spre noi relații pentru comandanți.

Provocările la care trebuie să facă față trupele de uscat sunt tot atât de dinamice ca și lumea în care trăim. Schimbările rapide aduse de cipurile de calculator și de progresele din domeniul telecomunicațiilor au afectat profund mediul nostru. Lumea este acum interconectată și interactivă. Mediul global informațional (GIE) evoluează zi de zi. Împreună cu progresul științei și cu forța calculatoarelor, GIE aduce avantaje enorme umanității în domenii ca: medicina, educația și industria. Acest mediu promite mult dar prezintă și noi sfidări, vulnerabilități și amenințări. În interiorul său nu există hotare politice sau teritoriale, ceea ce face ca „actele de război „ să capete caracter ambiguu.

Componentele întregii infrastructuri americane - finanțe, energie, educație, transporturi, telecomunicații, apărare și majoritatea aspectelor societății - sunt legate între ele și

interdependente. Departamentul Apărării se bazează pe rețelele comerciale de telecomunicații pentru mai mult de 95% din traficul său de informații. Acest lucru face SUA, în calitatea lor de principală țară a lumii, dependente de tehnologie, mai sensibile decât oricare alt stat la acțiuni adverse. Chiar și în cazul unui inamic slab, operațiile informaționale oferă un profit disproporționat de mare pentru orice investiție.

Progresul tehnologic nu face ca lumea să fie mai sigură și mai liniștită. Creșterea alarmantă a conflictelor regionale a dus la intensificarea tensiunilor și a făcut lumea mai complexă și mai instabilă. În plus, fanatismul unor secte continuă să producă destabilizare în întreaga lume Terorismul este mai sofisticat și ar putea implica folosirea unor arme de nimicire în masă și atacarea rețelelor de calculatoare și sistemelor care controlează rețeaua energetică națională, traficul aerian și alte infrastructuri importante. Chiar și un adversar mai puțin sofisticat care are foarte puțini bani poate obține sau chiar închiria o gamă largă de capacități în orice loc din lume. Tehnologii precum sistemul de poziționare globală (GPS), supravegherea prin sateliți, comunicațiile prin fibre optice, sistemele de emisie în direct, accesul la INTERNET, criptografia, sesizoarele și armele de precizie sunt cu toate disponibile în comerț. La preocupările legate de securitate se adaugă natura de sursă deschisă a GIE și faptul că ne bazăm pe acest mediu. Adversari potențiali ar putea obține acces la date importante și ar putea folosi mediul global informațional pentru a ne ataca.

În această lume a comunicațiilor globale, a sateliților, a imaginilor luate de sus și a CNN, indivizii din orice colț al lumii primesc informațiile aproape instantaneu. Aceste informații și relatări de presă afectează opinia națională și mondială, modelează acțiunile politicienilor și produc o contopire a nivelului tactic, operativ și strategie al războiului. Progresul tehnologic, relatarea informațiilor în mass-media și comprimarea relațiilor timp-spațiu contribuie la amplificarea raporturilor dintre nivelurile războiului, care îi ajută pe comandanți să vizualizeze fluxul logic al operațiilor, să aloce resursele și să încredințeze misiunile celui mai potrivit

comandament. Totuși, comandanții de la toate nivelurile trebuie să fie conștienți că, într-o lume a comunicațiilor directe, orice eveniment izolat poate să treacă prin toate cele trei niveluri. Relatările mass-media de astăzi ne măresc sensibilitatea atât față de pierderile proprii, cât și față de cele ale inamicului. Operația de capturare a dictatorului militar somalez Mohamed Farah Aidid din 03.10.1993 este un exemplu clar de contopire a celor trei niveluri de război. Imaginea de televiziune cu trupul unui soldat american târât pe străzile din Mogadiscio a produs aproape imediat o schimbare a politicii naționale. În acest caz a fost vorba de o misiune operativă, desfășurată într-un cadru tactic, cu ramificații strategice.

3.1. Tehnologia și dominația informațională

Valorificând inovațiile tehnologice, trupele constituie în prezent o forță de luptă bazată pe informație.Tehnologiile de informare îi pot oferi comandantului o înțelegere clară a situației sale curente în raport cu inamicul și cu mediul. Printr-o prelucrare deliberată și sistematică a volumului mare de date, se obțin informații care, sintetizate într-un tot coerent, asigură cunoașterea. Aceasta este cheia spre dominația informațională, un grad de superioritate informațională ce le permite comandanților să folosească INFOSYS și posibilitățile la dispoziție pentru obținerea avantajului operațional în lupta sau pentru controlarea situației în alte operații decât cele de război.

Țelul final al operației informaționale este de a-i face pe comandanții de unități apți să realizeze stăpânirea informațiilor, interzicând același lucru inamicului. Comandanții dobândesc această dominație informațională când cunoașterea situației proprii, a mediului și a inamicului potențial le oferă un avantaj distinct. Eforturile de informatizare a trupelor de uscat vor sprijini acest proces printr-o cunoaștere mai bună a situațiilor și prin vizualizarea câmpului de luptă, influențând profund conducerea luptei și desfășurarea tuturor operațiilor.

Dezvoltarea sistemelor de informare amplifică capacitățile comenzii și controlului (C^2) și eficiența armamentului. Avantajul

tehnologic de care ne bucurăm a îmbunătățit capacitatea de proiectare a forțelor și de sprijinire a acestora în operațiile executate la mare distanță. Prin concepte ca „logistică la timp" „adunare de la distanță" și „vizibilitate totală a dispozitivului", vom face ca să fie mai eficiente și să se poată susține. Toate aceste eforturi, exemplificate de inițiativa „Forța **XXI**" a armatei americane, se bazează în principal pe capacitatea de a valorifica o multitudine de noi sisteme de informare. Totuși sistemele sunt amenințate de aceleași vulnerabilități de care suferă sistemele civile când o organizație devine dependentă total de tehnologie. Vulnerabilitățile sunt exacerbate și de legătura acestora cu infrastructura civilă, și de faptul că se bazează pe aceasta.

3.2. Teoria informației informaționale

Operațiile informaționale constau din „operații militare continue în mediul militar informațional (MIE) care permit, întăresc și protejează capacitatea forțelor proprii de a culege, prelucra și folosi informațiile pentru a obține avantaje în toată gama de operații militare; operațiile informaționale includ interacțiunea cu mediul global informațional și exploatarea informațiilor inamicului și a capacităților sale de decizie sau interzicerea acestora".

Operațiile informaționale cuprind trei componente: operațiile; sistemele de informare; cercetarea, obținerea de date și culegerea de informații (RII).

Operațiile. Dimensiunea **operații** a operațiilor informaționale este compusă din toate măsurile, atât ofensive (atacarea C^2) cât și defensive (protecția C^2), folosite pentru obținerea dominației informaționale. Pe câmpul de luptă, aceste acțiuni sunt numite cu termenul de luptă în domeniul comenzii și controlului (C^2W). comandanții sincronizează elementele de luptă electronică (EW), măsurile de inducere în eroare a inamicului pe câmpul de luptă, operațiile de securitate (OPSEC), operațiile psihologice (PSYOP) și, dacă este necesar, distrugerea fizică și le concentrează împotriva sistemelor C^2 ale inamicului, personalului și materialelor, precum și asupra voinței și sprijinului populației adverse. În același timp,

comandanții trebuie să-și protejeze sistemele C^2 proprii de atacurile inamicului sau de exploatarea acestora de către inamic.

În timpul desfășurării operațiilor, afacerile publice (PA) și afacerile civile (CA) au un impact direct asupra operațiilor informaționale. Un plan coordonat de operație informațională care încorporează afacerile publice și afacerile civile este important pentru făurirea legitimității pentru națiunea-gazdă, pentru coaliție, pentru SUA și pentru sprijinul mondial, în special în alte operații decât cele de război. Afacerile publice trebuie integrate în operațiile informaționale pentru realizarea unei informări corecte, echilibrate și credibile. Activitățile de afaceri civile sunt importante pentru că realizează interfața cu organizațiile și cu indivizii importanți din mediul de informare. În fine, consilierii juridici analizează legislația internațională și internă și ajută la formularea unor reguli de angajare a operațiilor informaționale corespunzătoare conducerii desfășurării operațiilor.

INFOSYS. În mediul informațional actual, comandanții au nevoie de sisteme de informare robuste și de încredere pentru culegerea, prelucrarea și difuzarea volumului enorm de date în timp real pe tot globul. Operațiile informaționale includ sisteme de informare care obțin, produc, prelucrează și difuzează informații. O structură dinamică a INFOSYS este esențială pentru comandanți în scopul cunoașterii situației și al vizualizării câmpului de luptă. Aceste sisteme de informare afectează modul în care se desfășoară conducerea luptei. Viziunea asupra câmpului de luptă este întărită prin informatizare. Caracteristicile obiectivelor proprii și ale inamicului pot fi localizate și afișate pe display pentru comandanți, asigurându-le acestora actualizarea datelor situației curente. S-au dezvoltat sisteme de sesizoare pentru tragere care utilizează unde infraroșii sau milimetrice pentru **a vedea** și **a auzi** cu sesizoare acustice, **a simți** energia seismică, **a interpreta** informațiile culese, **a decide** dacă acestea percep o țintă pe baza unor criterii prestabilite și **a angaja** folosirea unor calculatoare miniaturale de mare viteză.

Cunoașterea situației de pe câmpul de luptă este dezvoltată într-o măsură fără precedent. Prin sisteme de informare moderne

și prin operații informaționale, comandanții vor fi capabili să gestioneze mai bine caracterul de incertitudine al războiului. În viitoarele operații terestre întrunite, coerența forței (și, astfel, aplicarea capacității de luptă) poate fi realizată mai degrabă printr-o bună cunoaștere a condițiilor de pe câmpul de luptă decât prin măsuri fizice de control tradiționale, cum ar fi măsurile grafice de control sau demarcarea geografică a zonelor de operații. Sistemele de informare viitoare vor avea atât componente militare secrete de sine stătătoare, cât și componente civile nesecrete. Securitatea acestor sisteme prezintă o importanță absolută pentru succesul operațiilor informaționale. Operația informațională are la bază faptul că persoana potrivită primește informația potrivită în locul potrivit.

3.3. Cercetarea, obținerea de date, culegerea de informații (RII).

Datorită dezvoltării tehnologice, trăim într-o lume a informațiilor. Un aspect critic al operațiilor informaționale este realizarea RII astfel încât să-i facă capabili pe comandanți să-și focalizeze eforturile. Aceasta este cheia pentru realizarea cunoașterii situației. Unul din obiectivele Forței XXI este de a folosi informațiile obținute pentru a realiza o viziune comună a câmpului de luptă la toate nivelurile și în timp real. Obținerea acestor informații nu este numai responsabilitatea organelor de cercetare. Pentru realizarea unui înalt nivel de fidelitate, comandanții trebuie să folosească toate mijioacele și sursele disponibile.

Cheia desfășurării operațiilor informaționale este pregătirea informativă exactă și la timp a câmpului de luptă (IPB).Conturarea operației informațională trebuie să depășească sfera tridimensională a câmpului de luptă și să cuprindă informații despre capacitățile, disponibilitățile și vulnerabilitățile tehnologiei. În plus, într-o lume interconectată, trebuie avut în vedere impactul pe care acțiunile noastre îl pot avea asupra sistemelor proprii și ale inamicului. Necesitățile de informare critice ale unui comandant pentru operația informațională le depășesc mult pe cele din trecut. Informarea trebuie să răspundă la următoarele întrebări:

1 - Cum funcționează sistemele de informare ale inamicului și care sunt vulnerabilitățile sale?

2 - Cum acționează ciclul de decizie al inamicului?

3 - Care sunt punctele sale nodale?

4 - Care sunt sursele sale de autoritate și de legitimitate?

5 - Cum funcționează societatea sa?

6 - Ce capacități de atacare a sistemelor aliaților are?

În măsura în care se schimbă necesitățile, trebuie să se schimbe și personalul de informații. Acesta trebuie să prelucreze acum informații din surse netradiționale, ca INTERNET și alte medii globale de informare. Coordonarea celor trei componente ale operației informaționale va genera un efort integrat pe deplin care ne va da posibilitatea să obținem dominantă informațională și avantaj operativ. Acestea sunt concepte integrate și căi sporite de abordare a conflictelor și a luptei în era informațiilor.

3.4. Potențialul operației informaționale

Operația informațională este desfășurată permanent pentru a descuraja agresiunea, pentru a-i asigura pe aliați sau pentru a constrânge inamicul, toate acestea în sprijinul intereselor națiunii proprii. Dacă este desfășurată destul de timpuriu și cu succes, operația informațională poate preveni conflictele, reduce pierderile sau stabiliza rapid condițiile. Pentru comandanți, operația informațională este un multiplicator de luptă. A ști unde, când și cum să dai lovitura decisivă inamicului, interzicându-i acestuia aceeași capacitate, reprezintă un avantaj fenomenal. Prin operația informațională se pot concentra rapid și eficient efectele.

În alte operații decât cele de război se poate aplica operația informațională pentru controlul situației. În operația JOINT ENDEAVOR din Bosnia, operația informațională a fost desfășurată 24 de ore din 24. Prin operația informațională, IFOR cunoștea întotdeauna unde se aflau și ce făceau facțiunile rivale. Acest lucru a făcut ca IFOR să poată controla situația în termenii săi. Interacțiunea constantă cu mass-media și mesajul de speranță trimis populației prin operațiile psihologice și afacerile civile au constituit elementele principale ale succesului în Bosnia. Acțiunile

operației informaționale desfășurată de IFOR au prevenit conflictele din acea regiune.

Obiectivele operației informaționale scot în evidență, de asemenea, noi modalități de gândire despre atacarea sau apărarea centrelor de gravitație. Folosind capacitățile neletale ale operației informaționale, se poate ataca un centru de gravitație pentru subminarea legitimității sau acțiunilor inamicului. Rezultatul final poate fi atât prevenirea escaladării conflictului, cât ci contribuția la o victorie decisivă.

Pe măsură ce guvernul, societatea și armata unei țări devin inexorabil legate prin dependența lor de diferitele infrastructuri de informare, apar noi vulnerabilități. Accentul operației informaționale se pune pe analiza nodală a vulnerabilităților principale proprii și ale inamicului. Operația informațională poate viza conducerea, procesul de luare a hotărârilor și C^2 ale inamicului, poate crea potențialul de a controla sistemul procesului decizional al adversarului și cauza chiar colapsul acestuia. Capacitățile de atac derivate din operația informațională și puterea cipurilor de calculator asigură posibilități de succes mai mari decât cele rezultate din folosirea armamentului cu energie cinetică.

În același timp, aspectele defensive ale operației informaționale sunt la fel de importante pentru protejarea propriilor vulnerabilități și centre de gravitație.

Măsurile ŒW, ca operațiile psihologice, lupta electronică și distrugerea, constituie factorii-cheie în executarea unei campanii de operații informaționale. Folosirea lor combinată, împreună cu capacități moderne de culegere a datelor, de supraveghere și de cercetare, îi asigură comandantului instrumente pentru o campanie managerială bazată pe o percepție reală, astfel încât poate încerca să influențeze emoțiile, motivele și raționamentul obiectiv al inamicului. Dacă reușește, campania operațiilor informaționale poate afecta conducerea inamicului sau sprijinul populației în așa măsură încât să anticipeze conflictul și să permită realizarea scopurilor fără a pune soldații americani în pericol.

Totuși, când lupta este inevitabilă, o operație informațională reușită va reduce în mare măsură pierderile pentru că vom avea

mai multe informații decât inamicul și vom putea controla ritmul conflictului. Acești factori sporesc viabilitatea și importanța operației informaționale în apărarea și promovarea intereselor SUA în lume.

Astăzi, comandamentele regionale dezvoltă variate opțiuni flexibile de descurajare (FDO) pentru a reduce tensiunea și a descuraja agresiunea înainte de izbucnirea ostilităților. Aceste metode includ sancțiunile economice, blocadele sau demonstrațiile militare de forță. Cu ajutorul operației informaționale comandanții pot dezvolta opțiuni flexibile de descurajare extinse dincolo de aceste metode mai tradiționale. Dată fiind proliferarea mediului global informațional, tehnicile operației informaționale pot deveni „opțiunea flexibilă de descurajare de prima mână" într-o criză. Exploatarea vulnerabilităților infrastructurii inamicului și afectarea procesului de luare a hotărârilor de către acesta se numără printre posibilele opțiuni flexibile de descurajare care ar ajuta la rezolvarea unei crize înaintea transformării acesteia în conflict armat. Astfel de acțiuni reclamă o coordonare strânsă și, cel mai probabil, o aprobare interagenții. În acest mod operația informațională va deveni o componentă integrală a capacităților noastre de proiecție a puterii.

Activitățile strâns coordonate și sincronizate ale afacerilor publice au devenit vitale în acest mediu. Afacerile publice corecte și oportune - în care comandanții sunt văzuți făcând tot ceea ce depinde de ei pentru a prezenta adevărul - sunt importante pentru desfășurarea operației informaționale și vor ajuta la descurajarea agresiunii, la liniștirea și sprijinirea aliaților și la obligarea celor cu care ne luptăm să ne accepte voința.

Definirea modului nostru de a lupta va depinde, în parte, de noi reguli de angajare în luptă. Acestea constituie o provocare însemnată pentru operația informațională.

Datorită caracterului articulat al mediului global de informare și folosirii în comun a platformelor de informare trebuie să se analizeze cu atenție modul în care să fie vizat sistemul de informare al inamicului, deoarece ceea ce se face ar putea avea impact asupra unor *terți neutri. O* altă situație grea ar putea avea loc dacă s-ar

hotărî neutralizarea unei rețele electrice care alimentează spitalele inamicului sau sistemele de control al traficului. Natura atotcuprinzătoare a INFOSYS va continua să influențeze dezvoltarea, limpezirea și dezbaterea regulilor de angajare a operațiilor informaționale atât în timp de pace , cât și de Război.

3.5. Organizarea desfășurării operațiilor informaționale ale trupelor de uscat

Pentru a concentra eforturile trupelor de uscat spre acest aspect important al luptei, gl. Reimer a declarat, în septembrie 1996, ca intenția lui este de a instituționaliza operațiile informaționale , care sunt vitale pentru modul în care trupele de uscat desfășoară operațiile. Pentru aplicarea în practică a acestei intenții, o serie de organisme răspund de integrarea operațiilor informaționale în trupele de uscat.

3.6. Triada pentru operațiile informaționale ale Statului Major al Departamentului Trupelor de Uscat (HQDA).

S-a stabilit o triadă constând din oficiile adjunctului șefului statului major pentru operații și planuri (DCSOPS) , adjunctului șefului statului major pentru informații (DCSINT) și directorului sistemelor de informare pentru comandă, control, transmisiuni și calculatoare (DISC4). Triada primește directive de la secretarul Departamentului Trupelor de Uscat și de la șeful Statului Major al Trupelor de Uscat și asigură unitatea eforturilor celor trei componente ale operațiilor informaționale. În cadrul triadei, punctul central este DCSOPS.

3.7. Comandamentul pentru Instruire și Doctrină al Trupelor de Uscat (TRADOC).

Comandantul Centrului Armelor întrunite de la Fort Leavenworth, Kansas, este cel care propune operațiile informaționale ale TRADOC. Centrul răspunde de dezvoltarea doctrinei operațiilor informaționale (FM 100-6), de instruire, de dezvoltarea conducerii, de problemele de organizare, materiale și

de Personal. Acum, după ce regulamentul FM 100-6 a intrat în vigoare, următoarea lui sarcină este de a dezvolta tactica, tehnica și procedeele (TTP) operațiilor informaționale. Viitorul manual pe această temă va prezenta modul de planificare și executare a operațiilor informaționale la nivel corp de armată și divizie. De asemenea, el este pe cale de a incorpora operațiile informaționale în programa și exercițiile diferitelor școli, inclusiv în Programul de pregătire a conducerii luptei (BCTP) pentru corpuri de armată și divizii și în exercitiul PRAIRIE WARRIOR pentru cursanții Colegiului de Comandă și Stat Major.

3.8. Activitatea de luptă informativă terestră (LIWA). Situat la Fort Belvoir, Virginia, LIWA este un organism important pentru implementarea operațiilor informaționale în trupele de uscat. Acesta repartizează echipele de sprijin în campanie (FST) pentru întărirea statelor majore de campanie ale comandanților și asigură experiența tehnică în materie de operații informaționale pe care statele majore nu o au. Echipele coordonează, planifică și sincronizează diferitele elemente ale operațiilor informaționale pentru a facilita executarea acestora în timpul operațiilor militare. Echipele de sprijin în campanie îi consiliază pe comandanți în privința operațiilor importante de atacare a comenzii și controlului inamicului și celor de protejare a comenzii și controlului propriu. O astfel de echipă a asistat trupele de uscat din Europa în elaborarea planului de protejare a comenzii și controlului pentru operația JOINT ENDEAVOR și a continuat să sprijine IF OR. Echipele LIWA acționează, de asemenea, împreună cu statele majore din componența trupelor de uscat în timpul exercițiilor importante și situațiilor de urgență reale din lume.

Cea mai nouă misiune a LIWA este înființarea unei echipe de reacție la problemele intervenite în rețelele de calculatoare ale trupelor de uscat (ACERT). Această echipă are capacitatea de a răspunde la situațiile de penetrare sau atacare a rețelelor protejate sau neprotejate. În cazul unor astfel de incidente, echipa va identifica problema, va institui controlul, va repara daunele aduse sistemului și va coordona măsurile contrainformative sau de sprijinire a întăririi legislației.

3.9. Necesitățile de pregătire în vederea operațiilor informaționale.

Dezvoltarea calităților necesare conducătorilor și militarilor pentru desfășurarea viitoarelor operații informaționale va necesita timp și resurse. În prezent, trupele de uscat au militari pregătiți pentru activități ale operației informaționale ca afacerile civile, operațiile psihologice și lupta electronică, dar puțini sunt cei care dispun de o bază sau de antrenament în ceea ce privește totalitatea conceptelor operației informaționale.

Oricine poate începe să devină competent în unele aspecte ale IQ, cum ar fi protejarea C^2. Managerii și utilizatorii sistemului au nevoie de pregătire nemijlocită privind bazele securității sistemului și rețelei. Trupele de uscat pregătesc cursurile necesare. Totuși, această instruire poate fi realizată printr-o varietate de alte surse. Chiar fără o pregătire formală, utilizatorii calculatoarelor - orice militar din forța informatizată a trupelor de uscat - pot ajuta la câștigarea războiului informațional. Lucruri simple ca protejarea parolelor, verificarea antivirus a dischetelor înainte de copierea fișierelor de pe acestea și supravegherea calculatoarelor pornite vor întări în mare măsură siguranța lucrului. Operațiile informaționale trebuie integrate în exercițiile de nivel unitate și în programa centrelor de instrucție de luptă.

3.10. Responsabilități ale conducerii operațiilor informaționale.

Comandanții pot să înceapă încorporarea operațiilor informaționale prin a cere statelor majore să se familiarizeze cu prevederile regulamentului FM 100-6. De asemenea, ei trebuie să pună două întrebări, și anume:

- are nevoie corpul de armată, divizia sau gruparea operativă – tactică de o celulă ad-hoc pentru operații informaționale?
- cum va integra eșalonul respectiv operațiile informaționale în planurile de urgență sau în exerciții?

3.11. Celula pentru operații informaționale - o variantă a unei astfel de celule ar trebui să cuprindă un ofițer cu IO/C^2W Asemenea funcție sau specialitate nu există în prezent, dar este

necesară. Ofiterul respectiv va trebui nu numai să aibă cunoștințe de bază privind toate aspectele IO si C^2W, și mai important, să fie capabil să sincronizeze operația informațională pentru a sprijini planul și intenția generală a comandantului. De asemenea, va trebui să se ceară o echipă de sprijin în campanie de la LIWA pentru a ajuta la planificarea și coordonarea operației informaționale.

4. OPERAȚIILE INFORMAȚIONALE PENTRU SITUAȚIILE DE URGENȚĂ

Deoarece operația informațională este aplicabilă atât în timp de pace cât și de război, următoarele exemple arată modul în care comandanții ar putea integra IO în planurile și operațiile pentru situații neprevăzute. Aceste exemple sunt principiale, dar dificultatea pentru comandanți constă în orchestrarea și armonizarea multitudinii de componente ale operației informaționale.

4.1. Dislocarea unui corp de armată în Orientul Mijiociu - misiune de impunere: împreună cu alte forțe întrunite și de coaliție din zonă, se întocmește un plan detaliat al C^2W pentru izolarea și subminarea conducerii inamicului; coordonarea interagenții, cu valorificarea mijioacelor naționale, este desfășurată pentru asigurarea unui plan integrat; analiza nodală a infrastructurilor inamicului este completată cu aceea a profilului personalităților din conducerea inamicului; o campanie de gestionare a percepției este prestată pentru a rupe orice coaliție pe care inamicul ar putea să o realizeze cu statele vecine; această campanie vizează și sprijinul populației pentru guvernul inamicului; în același timp, se desfășoară o puternică operație de a face publice pentru întărirea sprijinului intern față de acțiunile noastre; se fac evaluări de vulnerabilitate pentru identificarea deficiențelor sistemelor proprii astfel încât să putem proteja comanda și controlul; se iau măsuri de securitate întărită a infrastructurii forțelor armate de pe continentul american și a celor ce își au baza pe alte continente; toate acțiunile sunt sincronizate pentru a permite pătrunderea rapidă și fără opoziție în regiune, pentru stabilizarea zonei și reducerea riscurilor la adresa militarilor americani.

4.2. **Desfășurarea** unei divizii în Europa de Est - misiune de întărire a păcii: în cadrul unei misiuni a NATO, divizia își organizează o celulă IO în cadrul biroului G3 (operații); această celulă își centrează eforturile în direcția asigurării sprijinului informativ pentru legitimarea generală a implicării SUA în misiune și pentru realizarea stabilității în regiune; celulă IO primește date de la o varietate de elemente, printre care forțele speciale, contrainformațiile și alte mijioace de culegere a datelor din zonă, apoi folosește toate informațiile pentru a coordona acțiunile de afaceri publice și civile în zona de operații. În plus, personalul celulei asigură ca temele operațiilor psihologice și „mesajul" elaborat pentru operație să fie integrate în planurile sale. Mesajul operațiilor psihologice trebuie să fie elastic și energic pentru a promova o pace mai durabilă și stabilizarea regională. Comandantul diviziei stabilește necesitățile de informații critice privind fracțiunile aflate în luptă și protecția forței proprii; celula IO elaborează un plan de protejare a C^2 bazat pe o analiză a riscurilor la adresa diferitelor sisteme și rețele; pentru asigurarea succesului misiunii de întărire a păcii, celula IO trebuie să aibă permanent în vedere realizarea legitimării implicării forțelor americane.

4. 3. **Desfășurarea** unei brigăzi în Africa - misiune de asistență umanitară: o grupare operativă la nivel brigadă, aflată sub egida ONU, se desfășoară pentru a ajuta la realizarea operațiilor de ajutorare și pentru protejarea liniilor de aprovizionare a refugiaților; obiectivul operației de informare este nu numai de a sprijini acțiunile de ajutorare, ci și de a demonstra rolul pozitiv pe care îl au forțele americane în cadrul operației; comandantul grupării operative cere de la LIWA o echipă de sprijin în campanie pentru a ajuta la coordonarea planului IO; această echipă cooperează cu organele de informații pentru identificarea specificului culturii și populației locale, lucru care va ajuta la elaborarea unui plan IO viabil; esențială pentru succesul misiunii este coordonarea strânsă cu organizațiile neguvernamentale, cu partenerii de coaliție și cu fracțiunile combatante; planificatorii operației trebuie să aibă în vedere integrarea acestor grupuri în celula IO, este foarte

importantă stabilirea modului de realizare a legăturii cu ele într-o zonă în care mijloacele de comunicații interne sunt puține sau lipsesc cu desăvârșire; comandantul analizează cea mai bună modalitate de obținere a informațiilor pentru salvarea vieții refugiaților și urmărește să se realizeze activități de afaceri publice și civile solide.

Exemplele evidențiază doar parțial complexitatea operațiilor informaționale. Acestea reclamă analize intense și detaliate, planificare și coordonare. Totuși, exemplele scot în evidență unele considerații pe care comandanții trebuie să le evalueze pentru a optimiza capacitățile și misiunile operațiilor informaționale.

4.4. Implicațiile operațiilor informaționale

Operația informațională nu constituie un fel de „glonț de argint" pentru obținerea victoriei în viitoarele conflicte dar, așa cum sublinia președintele Comitetului întrunit al Statelor Majore, gl. John Shalikashvili: *„Proliferarea explozivă a tehnologiilor din domeniul informațional are un impact semnificativ asupra luptei în toate fazele sale, asupra întregii game de operații militare și asupra tuturor nivelurilor războiului"*. Astfel, importanța operațiilor informaționale nu trebuie exagerată. Ele constituie pentru comandanți un mijioc de asigurare a unui nivel de cunoaștere și de înțelegere a conducerii luptei niciodată atins până în prezent.

Într-o lume interconectată, bazată pe și pusă în mișcare de INFOSYS, necesitatea protejării infrastructurii și a cetățenilor noștri va constitui o provocare deosebită. Totuși, aceasta este o lume care poate fi exploatată în interesul nostru.

5. RĂZBOIUL MEDIATIC

Comunicarea de tip mediatic este expresia relevantă a democrației unui sistem politic, iar relația dintre ele este atât de strânsă și direct proporțională încât nici una nu poate fi concepută fără cealaltă. Astfel, cu cât structurile comunicării sunt mai cuprinzătoare și mai accesibile, cu atât există mai multe șanse potențiale de afirmare a democrației.

Expansiunea comunicării în general și mai cu seamă a celei de masă este determinată de cerințele informative și cognitive tot mai sporite ale individului, precum și de nevoia societății de autoreglare. Acești factori determinanți își subordonează instantaneu tehnologiile de vârf încât au reușit să plaseze fenomenul comunicării de masă în prim-planul vieții cotidiene, capacitatea tehnicilor multimedia de transmitere și redistribuire a informațiilor lărgind extraordinar atât sfera publicului, cât, mai ales, pe acea a resurselor de informare, documentare și divertisment. Altfel spus, implementarea *high-tech* în comunicare i-a conferit acesteia eficiența deplină, socializând-o de o manieră atât de masivă încât sintagma lui Marschall Me Luhan despre „satul global" aproape că nu mai exprima o realitate, ci o banalitate.

Nu numai că rapiditatea, diversitatea și volumul informației trebuie asociate cu libera circulație a informației, cu egalitatea accesului la informare și, nu în ultimul rând cu garantarea informării corecte a cetățeanului. Acestea, deși sunt principii înscrise în Declarația Universală a Drepturilor Omului, continuă a rămâne deziderate de împlinit pentru o viitoare ordine mondială, deoarece, ca și democrația, libertatea informației este acum, fără îndoială, inegal răspândită în lume. Mai mult chiar, ea rămâne tributară societății în care se manifesta, fapt subliniat, printre mulți alții, de profesorul Hervé Bourges: «Libera circulație prezintă toate defectele liberalismului economic. Aceasta înseamnă că ea se face în folosul celor mai puternici și în detrimentul celor slabi. *Laissez/dire, laissez paser* este legea junglei, în afara cazului când toți ar avea aceleași șanse și mijioace. Or, este limpede că șansele și mijioacele țărilor *lumii a treia*, în sfera informației sunt mult inferioare și că decalajele, ca și în celelalte domenii, continuă să se adâncească".

Prin urmare, dezechilibrul manifestat în propagarea informației nu are numai explicații istorice și tehnologice, ci este reflexul interesului și propagandei de sorginte economică, financiară și politică, manipulate cu abilitate de trusturile transnaționale de presă și nu numai. Acest dezechilibru este cultivat zi de zi de marile puteri politico-economice ale lumii în dauna țărilor mici și

mijlocii, pe coordonate biunivoce când se produce pe axa est-vest. Și univoce, întotdeauna dinspre nord înspre sud. Fapt ce se realizează aproape fără băgare de seamă, întrucât informația cu sens unic se insinuează perfid în conștiințele oamenilor, afectându-le cadrul de viață în cele mai diverse moduri, dar mai totdeauna cu efecte scontate.

În general, informația, fie ea politică, economică, culturală etc., este expresia interpretant coerente a realității complexe dintr-o anumită unitate de timp și dintr-un anumit loc. Ea concentrează un punct de vedere asupra lumii. Într-o oarecare măsură, valoarea informației este în strânsă legătură cu difuzarea ei. La baza acestei operații stă un proces complex de selecție și ierarhizare întemeiată pe criterii ideologice precise. Din puzderia de fapte și evenimente care dau substanță unei zile la scară planetară, marile agenții de presă, marile companii de radio și televiziune aleg 100-200 pe care le ierarhizează într-un anumit mod și apoi le difuzează. Desigur, este greu să pretinzi obiectivitate absolută în acest proces delicat și, în același timp, dificil, dar este inacceptabil ca el să fie transformat într-o metodă deosebit de subtilă de falsificare a realității, în conformitate cu interesele și ideologia promovate de ziariști și mijloacele de comunicare ce se erijează în principalele surse de informare „obiectivă" și „corectă" a lumii. Am folosit ghilimelele pentru obiectivă și corecte căci așa cum cineva a observat deja, în momentul de față aproape că nu mai există informație neutră ci numai „informație de luptă", adică avem de-a face cu transformarea tezei în informație prin deghizarea funcțiilor militante în funcții informative.

Odată ajunși aici se impune constatarea existenței unor centre de putere informațională interesate să dea „știrii", „comentariului" și imaginii direcția și conținutul conforme unor intenții și scopuri manifestate. Procedeul presupune utilizarea cu bună știință a unui arsenal de mijloace și tehnici de falsificare și manipulare a informației, care verificate și identificate de specialiști le pot furniza acestora argumente că se află în plin război mediatic, componența esențială a războiului psihologic. În principiul ei, au în vedere cinci posibilități strategice:

1. se acordă proeminență unor fapte fară importanță reală, nerelevante, în detrimentul celor cu adevărat importante, sau se amestecă nedistinct știrile nesemnificative cu cele semnificative.

2. difuzarea unor știri fragmentare în locul celor complete, sau asamblarea unor informații parțiale, pentru a crea impresia unui adevăr complet.

3. prezentarea știrilor într-o manieră care să conducă la interpretări și concluzii eronate, favorabile intereselor particulare.

4. înfățișarea evenimentelor într-un mod de natură să provoace îndoieli și temeri nejustificate sau chiar exagerate, cu intenția de a influența sau condiționa acțiunile ulterioare ale indivizilor, comunităților de orice tip, națiunilor sau guvernelor.

5. trecerea sub tăcere a faptelor, evenimentelor care se presupune că ar suscita anume reacții din partea publicului sau a altui destinatar, combinate, eventual cu supralicitarea altora, în dorința de a le estompa pe cele dintâi.

Este, dacă vreți, partea văzută a icebergului!

Partea ne văzută, covârșitoare este destinată superprofesioniștilor informației. Este câmpul de bătălie pe care se înfruntă și se desfășoară forțe atât de copleșitoare încât doar un război convențional poate fi invocat ca termen de comparație, dar și în acest caz numai pentru estimarea cheltuielilor materiale și mai puțin a rezultatelor politico-economice, de multe ori mult mai eficiente în cazul războiului informațional. Efectul său este devastator demoralizarea și inducerea ideii în mediile elitei jumalistice mondiale că informarea corectă a devenit imposibil de depistat - și cu atât mai puțin de utilizat și propagat - este cea dintâi și cea mai importantă bătălie câștigată de războiul mediatic. Este o victorie psihologică! Adică esențialul în orice tip de război! Restul... restul ține de tehnică, de tactică și strategie, de arta de a dirija pionii informaționali pe tabla de șah a acestui război ce se va sfârși doar o dată cu civilizația care i-a dat naștere și-l întreține zi de zi, ceas de ceas, minut de minut.

„Cea dintâi dintre forțele care conduce lumea este minciuna"; afirmă Jean-François Revel, unul dintre marii ziariști ai timpului nostru în deschiderea volumului *Cunoaștere inutilă*, volum prin

care dorește să demonstreze că într-o lume copleșită de minciună mediatizată, - cum brutal numește el dezinformarea -, a vrea sau a mai putea să înțelegi ceva din ce se întâmplă pe mapamond a devenit o întreprindere „inutilă", sortită de la bun început eșecului. Căci, proclama la rându-i Simone Weil: „Epoca noastră este atât de otrăvită de minciună încât transformă în minciună tot ce atinge. Și noi suntem ai epocii: nu avem nici un motiv să ne vedem mai buni decât ea".

Or, cum minciuna de dragul minciunii nu există, deoarece minciuna înseamnă „denaturarea intenționată a adevărului având de obicei ca scop înșelarea cuiva", rămâne de fiecare dată a ști să identifici sursa minciunii, interesul care a determinat „punerea ei la lucru" și, nu în ultimul rând „ținta și efectele scontate. Profesional vorbind, a identifica sursele și cauza dezinformării și a-i neutraliza efectele.

Întrucât în războiul mediatic dezinformarea deține locul strategie central, toate celelalte mijioace utilizate - precum intoxicarea, provocarea, propaganda, publicitatea dirijată - nefiind decât atributele sale factice, găsim esențială definirea sa cât mai exactă.

Se recurge la dezinformare deoarece se crede în puterea cuvântului și, în ultimul timp din ce în ce mai mult, a imaginii de a „disloca" inamicul. Spre deosebire de dezinformarea folosită în timp de război - preponderent militară - și de intoxicarea reciprocă a serviciilor secrete, în general permise și încadrate în sfera vicleniilor de luptă admise, dezinformarea pe timp de pace - cu precădere mediatică - are ca scop voința permanentă de „distrugere a întregului sistem de cunoaștere obiectivă a realității într-o societate data", cum remarca în 1984 C. Meinik.

Că dezinformarea a devenit o realitate cotidiană abia în timpul nostru ne-o dovedește faptul că până nu de mult dicționarele – inclusiv cele românești – nu cunoșteau decât accepțiunea comună reieșită prin alăturarea logică a vocabularelor *dez+informa*, adică „a informa (cu bună știință) în mod greșit". Termenul purtător al unei conotații speciale a fost introdus pentru prima dată după cel de-al doilea război mondial în Marea Enciclopedie Sovietică -

firește îmbibat de ideologia comunistă - iar în Dicționarul Academiei Franceze abia în 1984, unde are următoarea definiție:

„Acțiune intermitentă sau continuă - prin folosirea oricărui mijioc - ce constă în inducerea în eroare a unui adversar sau în favorizarea subversiunii în rândurile acestuia în scopul de a-l slăbi".

Chiar și așa explicația rămâne nesatisfacătoare, obligându-ne să apelăm la specialiștii în domeniu care cunosc dezinformarea în mod nemijiocit. Astfel, însuși părintele K.G.B.-ului, Dzerjinski, fixând misiunile și metodele C.E.K.A. stabilea încă din 1917 un sistem de ofensivă mediatică, destinat compensant forțelor armate sovietice: „Comuniștii trebuie să fie pregătiți să folosească la nevoie tot felul de șiretlicuri, planuri și stratageme ilegale, să nege și să ascundă adevărul. Politica comunistă vizează în mod concret învrăjbirea în rândurile inamicilor [...]. Cuvintele mele erau alese în așa fel încât să provoace ura și confuzia, nu pentru a convinge adversarul, și pentru a-l disloca; nu pentru a-i îndrepta greșelile, ci pentru a-l distruge măturându-i structurile de pe suprafața globului". (după John Barron, *K.G.B.*, Paris, 1975)

G. Veraldi, în prefața lucrării lui Pierre Nord, *L 'Intoxication*, apărută la Paris în anul 1971, indică scopul dezinformării pe cât de concis, pe atât de lămuritor:

„Crearea unei realități false atât de convingătoare încât adversarul să o creadă justă".

Iar celebrul sovietolog Alexandr Zinoviev reușește, în *Para Bellum*, să exprime superlativul în materie:

„Inamicul trebuie să acționeze așa cum dorim noi, spre folosul nostru, dar fiind convins că acționează conform propriei voințe, deci împotriva intereselor noastre".

Însă cea mai explicită și profesională definiție am aflat-o în volumul *Le temps de la desinformation* (Paris, 1986) de Henri-Pierre Cathala, apărut în traducere românească în 1991 cu titlul *Epoca dezinformării*, volum de autoritate în materie, care ne-a fost de un real folos în elaborarea prezentei comunicări și pe care îl recomandăm cu căldură tuturor specialiștilor ca pe un manual fundamental:

„Dezinformarea reprezintă ansamblul procedeelor dialectice puse în mod intenționat pentru a reuși <manipularea > perfectă a persoanelor, grupurilor sau a unei întregi societăți, în scopul de a le devia conduitele politice, de a le domina gândirea sau chiar de a le subjuga. Presupune disimularea surselor și scopurilor reale, precum și intenția de a face rău, printr-o reprezentare deformată sau printr-o interpretare tendențioasă a realității. Se înscrie în rândul acțiunilor psihologice subversive".

Plecând de la această definiție - cum, de altfel, este lesne de intuit - războiul mediatic presupune nu numai existența unor instituții și cadre specializate, dar mai ales alocarea de mijloace logistice excepționale, întotdeauna direct proporționale cu voința și gradul de implicare pe mapamond a forței politice sau economice respective. Pentru a ne face o imagine cât de cât lămuritoare asupra realității vom recurge la un pasaj mai detaliat din cartea lui Thiery Wolton, *K.G.B.-ul în Franța* (Paris 1986; București, 1992) referitor la ce înseamnă acest război pentru fosta U.R.S.S., cu convingerea că dacă amănuntele rămân valabile pentru timpul și locul la care se face referire precisă, esența aspectului poate fi avută în vedere, *mutatis mutandis*, pentru înțelegerea de principiu a unor realități similare:

„Patruzeci de miliarde de franci este cifra anuală de afaceri a unei întreprinderi ca *Michelin* sau o dată și jumătate suma de care dispune în fiecare an Ministerul Francez al Afacerilor Externe pentru a-și asigura funcționarea și a promova imaginea Franței în lume.

Patruzeci de miliarde este și suma pe care U.R.S.S. o cheltuiește anual pentru măsuri active și dezinformare, vârf de lance al războiului ideologie pe care-l duce împotriva țărilor democratice, pentru a le destabiliza.

Sintagma măsuri active a apărut în vocabularul sovietic în cursul anilor 1950 pentru a desemna un anumit număr de mijloace oficiale și clandestine puse în operă pentru a acționa asupra cursului evenimentelor, comportărilor și opțiunilor politice ale țărilor străine. Prin intermediul lor, U.R.S.S. încearcă să facă presiuni asupra deciziilor guvemamentale ale altor state, să

submineze încrederea populației în conducătorii ei și în instituții, să suscite tensiuni în relațiile internaționale, să-și discrediteze adversarii sau, în orice caz, să le slăbească pozițiile. *Măsurile active* prezintă în general o viziune deformată a realității pentru a înșela ținta, fie un guvern străin, fie cercurile politice sau opinia publică a unei țări.

Există două feluri de măsuri active. Deschise, atunci când acestea se aplică propagandei oficiale și relațiilor diplomatice normale: secrete, atunci când este vorba de propaganda clandestină, despre dezinformarea scrisă sau orală, despre activitatea agenților de influență și, în fine, despre organizațiile de masă subminate de sovietici.

În anii '80, măsurile active au devenit o prioritate pentru subversiunea sovietică, ca și spionajul științific și jefuirea tehnologiilor occidentale. Lupta împotriva dezinformării este deci esențială astăzi pentru însăși supraviețuirea democrațiilor. Dar în societățile noastre deschise și libere este adeseori foarte greu ca ea să fie combătută. Libera circulație a informației și dreptul oricui de a gândi, de a vorbi și de a scrie sunt sistematic utilizate de către U.R.S.S. pentru tulburarea opiniei publice și dezechilibrarea guvernelor occidentale.

Este adeseori dificil de făcut distincție între dezinformarea propriu-zisă și exprimarea opiniilor. Uniunea sovietică știe să se adăpostească în spatele acestei distincții pentru a-și difuza clandestin propaganda sau pentru a intoxica opinia publică prin intermediul agenților de influență complici (plătiți) sau pur și simplu manipulați (pe care Lenin îi numea deja *idioții necesari)* [...]. La Moscova, cel puțin două mii de persoane se ocupă numai cu măsurile active. Pentru a concepe, a planifica, a difuza dezinformarea, U.R.S.S. dispune de o organizație complexă, de o întreagă rețea în care fiecare fir este legat la cel mai înalt nivel, de Biroul Politic al partidului [...]. Secția Internațională administrează, coordonează și finanțează zeci de organizații de masă însărcinate cu manipularea opiniei publice mondiale, popularizând campaniile de propagandă elaborate de Moscova pentru susținerea obiectivelor sale politice: Consiliul Mondial al Păcii, Federația Sindicală Mondială, Organizația de

Solidaritate cu Popoarele din Africa și Asia, Federația Mondială a Tineretului Democratic, Uniunea Internațională a Studenților, Organizația Internațională a Ziariștilor, Conferința Creștină pentru Pace, Federația Internațională a Femeilor Democrate, Asociația Internațională a Juriștilor Democrați, Federația Mondială a Oamenilor de Știință" etc..

Este de la sine înțeles că pentru contracararea unei agresiuni de asemenea proporții statele occidentale și-au organizat servicii specializate pe măsură, servicii a căror dominantă doctrinară este preponderent „de acțiune", cum este cazul structurii înființate de președintele Herri Trumann în 1948, numită Office off Polyce Coordination, care în 1952 a devenit parte integrantă a C.I.A.. Despre acest organism se știe precis că are încredințate trei tipuri de misiuni:

I. Războiul psihologic (propagandă ocultă);

II. Acțiuni politice (contacte și fonduri secrete necesare pentru a acționa asupra situației politice dintr-o țară ostilă sau prietenă, ajungându-se până la diversiune);

III. Operațiuni militare limitate sau războaie neconvenționale.

Datorită faptului că dezvoltă o protecție deosebit de eficientă, organizarea și multe din acțiunile acestor structuri statale occidentale cu misiuni informative și contrainformative sunt foarte puțin cunoscute, mai ales în comparație cu K.G.B.-ul a cărei activitate a cunoscut un număr mare de defectori.

Deoarece în democrație opinia publică se formează pe baza presei, iar liderii nu pot acționa împotriva curentului opiniei publice, s-a ajuns la situația reală, constatată, printre alții, și de Michel Rocard că „Puterea mediatică este astăzi mai puternică decât puterea politică".

Într-o atare situație aproape că este inutil să mai precizăm că terenul, câmpul de luptă al războiului mediatic este tocmai opinia publică, prin agresarea conștiinței fiecărui cetățean de către colportorii de opinie - recrutați din rândul ziariștilor și al personalităților politice, economice, culturale, religioase etc.-, deveniți vehicule ale dezinformării, vectori ai minciunii.

Deși minciuna poate îmbrăca mii și mii de fațete, determinate

de cazuistica adusă în discuție, în esență există un număr limitat de „rețete" pentru instrumentarea informației tendențioase. Spre exemplu, Vladimir Voikoff, în lucrarea *Le Montage* (Paris 1982), considera că „repertoriul minciunii" nu conține mai mult de zece poziții.

Cu precizarea că în purtarea războiului mediatic informația distorsionată sau total falsă poate căpăta o varietate imensă de nuanțe, în principiu, și fără a-l considera restrictiv, suntem de acord cu acest „decalog al dezinformării", care identifică :

1. Abila combinare și dozare a jumătăților de adevăr cu jumătăți de minciună, primele determinând acceptarea celorlalte și aceasta cu atât mai ușor cu cât opinia publică este neutră sau deja paralizată.

2. Minciuna absolută, născocirea, adesea eficace datorită enormității sale ce poate seduce spiritele paradoxale și nu numai.

3. Contraadevărul - falsificarea la propriu de documente - neverificabil datorită lipsei de martori.

4. Minciuna prin omisiune, în special aceea care neglijează de a prezenta informația în întreg contextul ei, deturnând și trunchind datele reale.

5. Valorificarea informațiilor colaterale, a faptului întâmplător în detrimentul esențialului, estompat în mod savant.

6. Amestecarea faptelor, a opiniilor sau persoanelor echivalente, care, într-o anumită variantă, vor putea fi plasate cu ușurință într-un alt context, eventual incriminate, folosind o ilustrare adecvată, chiar dacă este abuzivă.

7. Recurgerea la informații reminiscente, indiferent dacă la origine ele au fost reale sau false, pentru a fi puse în contexte diverse sau realiza comparații nejustificate.

8. Minciuna înecată într-un noian de informații, existând posibilitatea de a fi regăsită ulterior pentru a servi drept punct de referință.

9. Citate aproximative sau trunchiate.

10. Forma superioară a minciunii, care înseamnă enunțarea adevărului, dar lăsându-se impresia că este minciună sau negarea unei afirmații în așa fel încât interlocutorul să creadă că, de fapt, o aprobă.

Acestora trebuie să le alăturăm, ca auxiliare, 5 mijloace subtile de dezinformare care, folosind capacitatea persuasivă a limbajului - capabil de nuanțări, ambiguități și inflexiuni -, acționează asupra auditoriului fără ca acesta să bage de seamă:

1. Afirmații făcute pe un ton angelic, dezinvolt sau indignat.

2. Exagerarea apocaliptică a unui fapt colateral, lipsit de importanță, în numele unor principii morale.

3. Slăbirea adevărului printr-o prezentare sarcastică sau persiflantă.

4. Manipularea abilă a vocabularului prin utilizarea unor termeni imprecișI, meniți a semăna confuzie, sau a trimite cu gândul la contexte străine subiectului prezentat dar cu conotație precisă în opinia publică.

5. Etichetarea interlocutorului atribuindu-i o pretinsă apartenență la un anumit sistem de idei, ce deviază atenția și poate fi respins mai ușor decât discutarea în detaliu a argumentelor veritabile prezentate.

Dar arsenalul războiului mediatic beneficiază de o forță pe cât de veche pe atât de eficientă și avantajoasă: **zvonul**. Se poate aprecia că este de neconceput existența unui mediu social-politic în care să nu existe zvonuri. Mai mult chiar, politică fară zvonuri nu se face. Zvonul este în esență o afirmație pe marginea afirmației oficiale. Este o contraputere, motiv pentru care proliferează pe terenul cuceririi gestionării puterii.

Unul dintre cei mai buni analiști contemporani din perspectivă politico-sociologică ai zvonului este Jean-Noel Kapferer. În lucrarea intitulată „Zvonurile - cel mai vechi mijioc de informare din lume" (Paris, 1990; București, 1993), acesta avansează următoarea definiție: „Vom numi așadar zvon apariția și circulația în cadrul societății a unor informații fie încă neconfirmate public de către sursele oficiale, fie dezmințite de acestea. «Se spune» este o «nonspunere», fie că zvonul devansează sursa oficială, fie că o contrazice."

Zvonul evită dezvăluirea identității surselor: alții vorbesc în

locul nostru, făcându-se purtătorii voluntari sau involuntari ai zvonului. Sursa rămâne învăluită în mister fără a putea fi identificată. Nimeni nu-și asigură responsabilitatea, dar toți sunt la curent. Zvonul nu are nevoie de dovezi căci opinia publică întemeindu-se mai mult și de obicei, nu atât pe fapte cât mai ales pe impresii, acuzația este de ajuns.

Așa cum este știut, zvonurile pot fi spontane sau elaborate, reale sau false. Pentru războiul mediatic sunt de luat în considerare cu precădere cele elaborate, care implică vehicularea a neadevărurilor totale sau parțiale. Răspândirea și dirijarea lor presupune abilități speciale, căci trebuie să te ferești să faci afirmații ofensante. Se pun întrebări insinuante, păstrând aparența de impartialitate, pentru a determina apariția îndoielii. Se sugerează ipoteze, lăsând publicului sau interlocutorului direct dreptul de a trage concluzii. Se enunță o enormitate, adăugându-se imediat că este îndoielnică dar.... Cine știe poate...

Este de la sine înțeles că zvonurile sunt răspândite în medii considerate propice, iar difuzarea lor trebuie să se facă simultan către mai multe ținte deodată, în așa fel încât ivirea zvonului din mai multe izvoare să conducă la confirmarea lui.

Alegerea mesajelor este fundamentală, fiind de preferat o insinuare comportând o parte de adevăr, dar sugerând o interpretare peiorativă, defăimătoare. Este indicat să se lanseze în cadrul unei discuții între ținte deodarece, dacă va exista un schimb de argumente, se vor găsi întotdeauna indivizi care, fie și numai din spirit de contradicție sunt gata să susțină veridicitatea calomniei știrii.

În cadrul zvonului un loc aparte îl ocupă calomnia. Insinuările privitoare la viața particulară aduc întotdeauna folose mari deoarece puțini oameni, în afara celor apropiați victimei și, în consecință, suspecți de părtinire sunt în stare să dezmintă calomnia. Este de reținut faptul că avantajul acestui gen de operații constă în aceea că pune victima în postura de acuzat și îi impune căutarea de probe pentru dezvinovățire. Victima trebuie să facă dovada nonexistenței faptelor incriminate ceea ce este, practic, imposibil, având în vedere că prin definiție, ceea ce nu există nu lasă urme.

Contrar unei idei răspândite, în viața publică nu trebuie niciodată să tratezi calomnia prin dispreț și tăcere. Întotdeauna vor exista indivizi bine intenționați capabili să o reînvie la momentul oportun. Adesea, calomnia este o operație în doi timpi: mai întâi se aruncă informația falsă, fără a părea că i se acordă atenție, urmând să fie apoi reluată cu referire la prima sa publicare.

Ca mijloc de protecție și de neutralizare a calomniei apelul la încredere nu servește la nimic, deoarece dezinformatorul se situează de la bun început pe o poziție favorizantă. De aceea se impune ca fără întârziere să se treacă la contraatac, cerându-se precizări cu privire la faptele incriminate, să fie solicitate dovezi palpabile referitoare la acuzație și originea sa și, mai ales, să fie deschis un proces de defăimare. Apoi vor trebui declanșate aceleași măsuri împotriva agenților de influență, indiferent dacă aceștia sunt sau nu complici conștienți ai dezinformatorului, pentru a-i discredita, intimida și neutraliza.

Totuși, în foarte multe cazuri, este dificil să se răspundă unei dezinformări mediatizate. Dezmințirea, chiar dacă este întotdeauna necesară nu este suficientă. După ce și-a lansat contra-adevărul, mai ales dacă se poate prezenta ca fiind un simplu transmițător a unei informații venite de aiurea, mincinosul nu are altceva de făcut decât să tacă și să aștepte. Minciuna reprezintă, practic un proces cu trei personaje. În afara „mincinosului" mai există cele două victime ale procedeului: cea asupra căreia acționează, și care încearcă fără prea mari șanse de izbândă să facă dovada bunei sale credințe, și cea care recepționează minciuna. Aceasta din urmă, indiferent dacă este o persoană sau însăși opinia publică, nu are posibilitatea de verificare, situându-se, fără să vrea, în postura unui fel de arbitru, judecător al diferendului ce-l opune pe „mincinos" victimei sale.

Împotriva dezinformării mediatizate nu se poate lupta fără un personal calificat, dispunând de mijloace adecvate și, în special, fără o direcție strategică și tactică care să fixeze scopuri clare și să coordoneze acțiunile necesare. Aceasta începe, ca în orice alt domeniu, prin identificarea și cunoașterea exactă a pericolului.

Că ne place sau nu, războiul mediatic nu mai trebuie tratat

superficial. El reprezintă forma vicleană a războiului total și, chiar dacă regulile pot evolua în funcție de circumstanțe, se supune unor principii fundamentale ce nu pot fi subestimate fără riscul înfrângerii. Nu este deloc prea mult spus dacă afirmăm că, bine condus, războiul mediatic poate determina capitularea unei națiuni în eventualitatea unui atac militar sau ideologie, prin pervertirea spiritului, inversarea ierarhiilor socio-culturale locale, reușite care induc populației o stare de indiferență, diminuându-i și derutându-i capacitatea de înțelegere și aderență la real.

De aceea lupta împotriva dezinformării nu reprezintă un domeniu izolat în care confruntarea se poate desfășura fără a ține seama de celelalte imperative ale apărării. Ea poate constitui faza preliminară și indispensabilă a unor negocieri diplomatice. Poate fi un factor important în reușita unor tranzacții economice de amploare. Este o necesitate pentru a putea rezista unei agresiuni psihologice împotriva națiunii, fie că este vorba de o campanie destinată modelării opiniei publice într-o problemă cheie, fie că vizează degradarea lentă și progresivă a sistemului de valori recunoscut și demoralizarea indivizilor.

Orice încercare de apărare în cadrul războiului mediatic trebuie să se desfășoare în conformitate cu un plan general, care să aibă fixate cu precizie obiectivele și responsabilitățile. Trebuie refuzate *„deplano"* toate inițiativele solitare.

De asemenea, apărarea împotriva dezinformării este formal interzisă amatorilor. Prea adesea s-au văzut factori politici responsabili sau comandanți militari care, crezând că sunt fini psihologi, au fost manevrați și depășiți de către adversar mult mai competent.

În aceste condiții trebuie arătată o grijă deosebită formării specialiștilor în domeniu, cerință obligatorie și necesară care solicită timp și atenție, precum și o gândire fără prejudecăți. Selecționare de cadre cu însușiri native, cum ar fi sângele rece, inteligența, perspicacitatea, răbdare, subtilitate etc., etc., care vor trebui să învețe și să-și însușească numeroase cunoștințe din domenii foarte diverse, în baza unei bune programe de instruire și a studiului aprofundat. Neapărat, acești specialiști vor trebui să

acumuleze o experiență practică, însă fară a pune în pericol, prin încercări intempestive, societatea pe care sunt chemați să o protejeze.

Nu trebuie scăpat din vedere faptul că în domeniul războiului mediatic orice acțiune, inclusiv aceea de a pregăti și forma un personal specializat, constituie un act de război și poate determina o contra-acțiune inamică. În plus trebuie adăugat faptul că într-o societate deschisă cum este a noastră vor exista întotdeauna spiritele nobile - în sensul pur al cuvântului - sau naivi care să denunțe cu vehemență însăși existent războiului mediatic, a luptei psihologice. Sensibilizarea, pregătirea și informarea prealabilă a publicului sunt indispensabile oricărei acțiuni. Aceste misiuni aparțin celor care guvernează și mijioacele de informare în masă care trebuie, în primul rând, convinse.

Pentru reușita în lupta de neutralizare a războiului mediatic un factor esențial îl reprezintă conștiința fiecărui cetățean. Aceștia nu pot rămâne simpli spectatori, așa cum ar fi posibil, la nevoie, în situația confruntărilor cu caracter militar sau economic. Este vorba de un domeniu în care „consensul", adesea invocat, însă rareori realizat, reprezintă un imperativ național absolut. Apărarea împotriva dezinformării nu se va putea realiza fără participarea generală a celor ce-i sunt victime. Imposibilitatea de a mai încredința altora grija pentru securitatea proprie constituie pentru cetățenii noștri o situație nouă, căreia nu-i vor putea face față de pe o zi pe alta.

„Consensul" național este, în mare măsură, determinat de încrederea pe care cetățenii o acordă statului ce-i guvernează. În acest context, trebuie să constatăm că micile șiretlicuri folosite în politica internă, cărora nici un guvern democratic din nici o țară nu le poate rezista, riscă să coste foarte scump națiunea pe planul apărării moralului. Încrederea nu este un capital din care să se poată consuma la cerere: ea exista sau nu. În democrații, toți indivizii obișnuiți vor trebui să învețe ce este aceea francheță și loialitate dacă vor să supraviețuiască.

Această necesară sporire a moralității vieții politice democrate ar putea fi una dintre consecințele neașteptate ale războiului

mediatic. Căci ne putem pune problema care va fi evoluția raportului de forțe dintre regimurile care practică o obiectivitate reală, deci urmate clar de popoarele lor, si cele ce se vor încăpățâna să continue a trișa cu ideile și faptele. Minciuna guvernanților va duce cel mult la pasivitatea supușilor și la reticența executanților, ceea ce nu facilitează deloc confruntarea cu realitățile lumii. Originalitatea războiului mediatic constă tocmai în faptul că atitudinea de sinceritate nu este determinată de cauze etice, ci de realism și necesitate.

6. RĂZBOIUL ELECTRONIC

Impactul mediului electromagnetic asupra capabilității operaționale a forțelor militare, echipamentelor, sistemelor și platformelor este atribuit efectelor mediului electromagnetic, care cuprinde **toate disciplinele electromagnetice,** precum compatibilitatea și interferența electromagnetică, protecția electronică, riscurile radiației electromagnetice asupra mijioacelor și materialelor volatile, precum și efectele fenomenelor naturale - fulgerul și precipitațiile. Echipamentele și sistemele care operează pe principiile electromagnetismului sunt caracterizate de **vulnerabilitatea electromagnetică** care le cauzează incapacitatea de a îndeplini misiunea stabilită, ca urmare a efectelor mediului electromagnetic.

În operațiile militare, termenul de **război electronic** *cuprinde ansamblul acțiunilor militare care implică utilizarea energiei electromagnetice pentru a determina, exploata, contracara, reduce și preveni acțiunile ostile în spațiul electromagnetic, precum fi măsurile care asigură desfășurarea în siguranță a trupelor proprii și/sau aliate.*

Războiul electronic are trei componente principale: atacul electronic, protecția electronică și sprijinul electronic.

• **Atacul electronic.** Atacul electronic este componenta războiului electronic care implică utilizarea energiei **electromagnetice, a energiei dirijate sau a armelor antiradiație** pentru a ataca mijloacele, echipamentele sau personalul, cu intenția de a

degrada, neutraliza sau distruge capabilitățile de luptă ale inamicului ci este considerată o formă de luptă. Atacul electronic include:

- acțiunile întreprinse pentru a preveni sau reduce utilizarea cu eficiență de către inamic a spectrului electromagnetic, cum ar fi bruiajul și înșelarea electronică;

- utilizarea armelor care folosesc energia electromagnetică sau energia dirijată ca principal mecanism distructiv (laseri, arme dirijate pe fasciculul de radiofrecvență sau fascicule de particule cu energie înaltă).

• **Protecția electronică.** Protecția electronică este o componentă a războiului electronic care implică aplicarea de măsuri active și pasive pentru **protecția personalului, mijloacelor și echipamentelor** la efectele utilizării războiului electronic de către forțele proprii sau inamice.

- **Sprijinul electronic.** Sprijinul electronic este componenta războiului electronic implicată în acțiunile întreprinse pentru **a căuta, intercepta, identifica și localiza sursele de radiație intenționată sau neintenționată a energiei electromagnetice,** în scopul recunoașterii imediate a unei amenințări, combaterii acesteia, planificării și conducerii operațiilor viitoare. Sprijinul electronic asigură informațiile necesare luării deciziei de implicare a războiului electronic în operații sau alte acțiuni tactice cum ar fi evitarea amenințării, stabilirea țintelor și dirijarea. Datele de sprijin electronic pot fi utilizate pentru a furniza informații privind semnale *(SIGINT),* pentru stabilirea țintelor atacului electronic sau pentru distrugerea fizică și pentru măsurarea parametrilor și determinarea amprentei semnalelor *(MASINT).* SIGINT poate contribui la estimarea rezultatelor atacului și pe această bază, la modificarea planului operațional general.

Acțiunile de război electronic sunt executate în tot spectrul electromagnetic pentru **a asigura și menține controlul și utilizarea eficientă a acestuia** de către forțele proprii și pentru a interzice utilizarea lui de către forțele inamicului prin modificare, distrugere, intrerupere sau înșelare. Necesitatea controlului spectrului electromagnetic și tipul de acțiuni de război electronic necesare

pentru controlul acestuia sunt dictate de mediul operațional în care se desfășoară acțiunile militare.

Loc și rol

Principalul rol al acțiunilor de război electronic este de a câștiga confruntarea în spațiul electromagnetic cu sistemele electronice a căror activitate poate fi, după caz, potențial ostilă sau ostilă.

Pe timp de pace, rolul războiului electronic este de a identifica și dimensiona factorii de risc și amenințările la adresa securității și apărării naționale, specifice spațiului electromagnetic, precum și realizarea unei capacități de descurajare și reacție credibilă, adecvată tuturor situațiilor probabile.

În situații de criză, rolul războiului electronic este de a supraveghea spațiul electromagnetic din zonele de crize, în cooperare cu celelalte forțe implicate pentru gestionarea și rezolvarea acestora.

La război, rolul războiului electronic este de a diminua potențialul de luptă inamic concomitent cu multiplicarea capacităților de acțiune a forțelor proprii prin câștigarea confruntării în spațiul electromagnetic, conform concepției operației.

În operațiile întrunite, războiul electronic reprezintă una din capabilitățile militare care sunt **integrate în operațiile informaționale.**

Deoarece poate afecta colectarea, procesarea, păstrarea și transmiterea informațiilor bazate pe energia electromagnetică, **războiul electronic reprezintă o componentă esențială a operației informaționale.** Războiul electronic are, de asemenea, un rol important în **suprimarea apărării antiaeriene a inamicului *(SEAD).***

Acțiunile principale de război electronic

Principalele acțiuni de război electronic au apărut de-a lungul timpului pentru **a exploata oprtunitățile și vulnerabilitățile inerente în fizica energiei electromagnetice.** În acest sens

continuă dezvoltarea de noi echipamente și tactici, deși fizica energiei electromagnetice rămâne constantă. Aceasta este rațiunea pentru care acțiunile de bază ale războiului electronic rămân eficace în pofida schimbării echipamentelor și tacticilor.

Principalele acțiuni desfășurate în cadrul războiului electronic sunt:

6.1. Compatibilitatea electromagnetică

Compatibilitatea electromagnetică *(EMC)* reprezintă capabilitatea sistemelor, echipamentelor și componentelor care utilizează spectrul electromagnetic de a funcționa în mediile operaționale destinate **fără a suferi sau produce degradări inacceptabile** din cauza radiației sau reflexiei electromagnetice. Compatibilitatea electromagnetică implică: aplicarea strictă a gestionării spectrului electromagnetic; proiectarea sistemelor, echipamentelor și componentelor care să asigure funcționarea acestora fără interferențe; concepte și doctrine clare care să crească eficiența operațională.

6.2. Dezinformarea electronică

Dezinformarea electronică reprezintă radierea deliberată, reradierea, denaturarea, suprimarea, absorbția, interzicerea, amplificarea sau reflexia energiei electromagnetice în mod intenționat **pentru a induce în eroare inamicul** sau sistemele de arme ale acestuia, care utilizează energia electromagnetică, având drept consecință diminuarea sau neutralizarea capabilităților de luptă ale inamicului. Dezinformarea electronică se prezintă sub următoarele forme:

– **Dezinformarea electronică manipulativă.** Acest tip de dezinformare implică acțiuni de eliminare a indiciilor de demascare relevanți care pot fi utilizați de către inamic, precum și transmiterea unor indicii false.

– **Dezinformarea electronică simulativă.** Acest tip de dezinformare implică acțiuni de simulare a capabilităților forțelor și mijloacelor proprii pentru a induce în eroare forțele inamicului.

• **Dezinformarea electronică imitativă.** Acest tip de dezinformare induce energie electromagnetică în sistemele electronice ale inamicului care imită emisiile acestuia.

6.3. Robustizarea electromagnetică

Robustizarea electromagnetică constă în acțiunile întreprinse pentru protejarea personalului, echipamentelor și infrastructurii împotriva efectelor nedorite ale energiei electromagnetice, prin **filtrare, atenuare, împământare și ecranare.**

6.4. Interferența electromagnetică

Interferența electromagnetică (EMI) reprezintă orice perturbare care **întrerupe, obstrucționează, modifică sau limitează performanțele** echipamentelor electrice sau electronice. Aceste perturbații pot fi induse intenționat ca în forme ale războiului electronic sau neintenționat, ca urmare a emisiilor secundare, precum și ca urmare a fenomenului de intermodulație.

6.5. Penetrarea electromagnetică

Penetrarea electromagnetică reprezintă introducerea intenționată prin diferite metode a energiei electromagnetice în calea de transmitere, în scopul **inducerii în eroare a operatorilor sau pentru a provoca confuzie.**

6.6. Bruiajul electronic

Bruiajul electronic reprezintă radiația deliberată, reradiația sau reflectarea energiei electromagnetice pentru a **preveni sau reduce folosirea eficientă a spectrului electromagnetic de către inamic** în scopul diminuării sau neutralizării capabilităților de luptă ale inamicului.

6.7. Impulsul electromagnetic

Impulsul electromagnetic reprezintă un impuls foarte puternic cauzat cel mai adesea de o explozie nucleară care afectează sistemele electrice și electronice, producând defectarea acestora prin intensitatea mare a curentului indus și supravoltaj.

6.8. Mascarea electronică

Mascarea electronică reprezintă **radiația controlată a energiei electromagnetice pe frecvențele proprii** astfel încât să se asigure protecția emisiilor proprii împotriva măsurilor de sprijin electronic sau SIGINT ale inamicului, fără a afecta semnificativ lucrul sistemelor proprii.

6.9. Stimularea electronică

Stimularea electronică reprezintă **radiația intenționată**

destinată a fi indusă în sistemele și componentele electronice ale potențialului inamic pentru a le determina să reacționeze, cu scopul de a cunoaște capabilitățile operaționale și acționale ale acestora.

6.10. Recunoașterea electronică

Recunoașterea electronică reprezintă **descoperirea, localizarea, identificarea și evaluarea radiațiilor electromagnetice.**

6.11. Cercetarea electronică

Cercetarea electronică (ELINT) reprezintă **cercetarea tehnică și localizarea radiațiilor electromagnetice noncomunicații** emise de alte surse decât exploziile nucleare sau radioactive.

6.12. Securitatea electronică

Securitatea electronică reprezintă protecția rezultată ca urmare a aplicării tuturor măsurilor destinate **interzicerii accesului persoanelor neautorizate la informații de valoare,** prin interceptarea și studierea radiațiilor electromagnetice noncomunicații.

6.13. Reprogramarea acțiunilor de război electronic

Reprogramarea acțiunilor de război electronic reprezintă **schimbarea sau modificarea intenționată a acțiunilor de război electronic sau a sistemelor de senzori** ca răspuns la schimbările produse în mediul electromagnetic, echipamente și tactici. Aceste schimbări pot fi rezultat al acțiunii deliberate a forțelor proprii, inamicului sau a unei terțe părți, ori pot fi determinate de interferența electromagnetică sau alte fenomene aleatoare. Scopul reprogramării acțiunilor de război electronic este acela de a menține sau îmbunătăți eficacitatea acțiunilor de război electronic și a echipamentelor sistemelor de senzori. Reprogramarea acțiunilor de război electronic include schimbările din sistemele de auto apărare, sistemele de arme ofensive și sistemele de informații.

6.14. Controlul emisiei

Controlul emisiei ***(EMCON)*** reprezintă utilizarea selectivă și controlată a emițătorilor electromagnetici, acustici sau de altă

natură, în scopul **optimizării capabilităților de comandă și control** (C2), simultan cu minimizarea, în folosul securității operațiilor a:

- detectării de către senzorii inamicului;
- interferenței reciproce între sistemele proprii;
- factorilor care împiedică executarea planurilor proprii de dezinformare militară.

6.15. Gestionarea spectrului

Gestionarea spectrului implică planificarea, coordonarea și administrarea utilizării spectrului electromagnetic prin proceduri operaționale, administrative și tehnice. Obiectivul gestionării spectrului electromagnetic este de a permite sistemelor electronice să lucreze la posibilitățile maxime în mediul dat, fără a produce sau suferi interferențe inacceptabile.

6.16. Regimuri de lucru de rezervă

Regimurile de lucru de rezervă *(WARM)* reprezintă caracteristicile și procedurile de operare ale senzorilor, sistemelor de comunicații, navigație, recunoaștere, a celor de arme, precum și a sistemelor de contraacțiune, **care vor contribui la creșterea eficacității acțiunilor militare dacă nu sunt cunoscute sau înțelese de către inamic** înainte de a fi utilizate, dar care pot fi exploatate sau neutralizate dacă sunt cunoscute anterior. Regimurile de lucru de rezervă sunt păstrate în mod intenționat în rezervă pentru situații de criză sau în caz de război.

Așadar, având în vedere că în prezent mijloacele electronice sunt utilizate atât de organizațiile militare cât și de cele civile pentru **comunicații, navigație, ca senzori, pentru păstrarea și prelucrarea informațiilor,** putem concluziona că utilizarea mediului electromagnetic crează **vulnerabilități și oportunități pentru războiul electronic,** iar forțele armate fac tot posibilul pentru a profita de acest aspect în sprijinul operațiilor militare.

7. TERORISMUL INFORMATIC

Terorismul informațional se poate defini în contextul războiului informațional, cât și într-acela al terorismului convențional.

Într-un efort de a atrage atenția publicului, teroriștii politici își săvârșesc propriile acte utilizând mijloacele de informare în prim planul strategiilor lor, bazându-se pe presupunerea că accesul la structura de comunicații este legat de putere. Cei care cred în această presupunere ar putea viza sistemele informaționale digitale în urmărirea obiectivelor politice.

Infrastructura informațională sprijină transferurile de informații militare, financiare și comerciale de către consumatori sau în interesul unor state. Luând în considerare prezența computerului în societatea modernă, nu este surprinzător că în trecut teroriștii au vizat uneori sistemele de computere, în Japonia unele grupuri au atacat sistemele de control computerizat al trenurilor de navetiști, paralizând câteva ore cele mai importante orașe; manifestul Brigăzii Roșii italiene stipula că distrugerea instalațiilor și a sistemelor de computere reprezenta un obiectiv pentru „a lovi în inima statului". Mai recent, suporterii Sinn Fein de la Universitatea Austin din Texas au expus pe Internet detalii sensibile despre instalații ale serviciilor militare de informații britanice și despre secții de poliție din Iranda de Nord.

[Pe măsură ce tehnologia devine tot mai accesibilă, disponibilitatea și potențialul acesteia cresc, în timp ce costurile financiare și celelalte costuri scad, teroriștii putând deveni mai orientați pe tehnologie în tacticile și strategiile lor. Cele mai vulnerabile la a fi atacate sunt sistemele automatizate, cele care depind într-o mare măsură de ultimele tehnologii, avansul tehnologic prezentând dezavantajul că, în eventualitatea în care o tehnologie conține greșeli de proiectare, pagubele rezultate sunt direct proporțional cu valoarea respectivei tehnologii. În același timp trebuie avut în vedere că pe măsură ce un sistem este tot mai complex, posibilitățile de apariție a unor erori cresc.]

Avioanele comerciale, conductele de gaz natural, rețeaua de energie electrică, platformele marine de foraj, precum și înregistrările de date de pe sistemele de stocare ale organizațiilor guvemamentale sau ale anumitor corporații reprezintă exemple de obiective expuse sabotajului, ale căror distrugeri ar avea efecte implicite de intensitate mult mai mare decât pierderile principale pe care acestea le-ar putea sugera...

În prezent, mai degrabă decât să atace un anumit obiectiv bine protejat sau să încerce operațiuni care să implice rezultate cu grad (potențial) ridicat de risc, teroriștii vor căuta și vor exploata vulnerabilități încă neidentificate până acum și, pur și simplu, își vor adapta corespunzător planul de atac și prioritățile tactice.

Includerea tehnologiei informației în cadrul complexului militaro-industrial, precum și proiectarea și implementarea strategiilor de război informațional pot, de asemenea, să atragă teroriștii spre utilizarea tehnologiei computerelor.

[În prezent, în cazul României, riscurile expunerii la eventuale atacuri ale unor teroriști informaționali sunt scăzute, datorită „avantajului" oferit de inexistența unor sisteme integrale care să rezolve funcțiuni vitale, de interes național și, probabil, datorită dezinteresului prezentat de cyberspațiul autohton.]

Se încearcă, în continuare să se ofere o definiție a terorismului informațional, plecând de la definirea războiului informațional. Un act de violență politică, exercitat de către oricine altcineva decât un membru al unor forțe armate ale unui stat legitim, este tratat adesea drept un act de terorism. Această abordare este, însă, doar rareori corectă, dar conotația subversivă și criminală a termenului „terorist" a reieșit și din multe acțiuni în care s-a abuzat de utilizarea computerelor, acestea fiind etichetate drept „terorism informațional".

Politica și metodologia de contracarare a acestor acte criminale depinde într-o mare măsură de motivațiile făptuitorilor; prin urmare sunt necesare definiții mai clare și mai concise asupra „terorismului informațional", dacă acesta trebuie să fie luat în calcul de către politica de securitate națională.

Terorismul politic reprezintă folosirea sistematică a violenței fizice actuale sau care se întrevede pentru atingerea unui obiectiv politic, pentru a crea un climat general de teamă publică și de destabilizare a societății, influențând astfel populația sau politica guvernamentală.

Terorismul informațional reprezintă legătura dintre acțiunile criminale de abuz sau fraudare a sistemelor informaționale și violența fizică a terorismului. Prin urmare, în special din punct de

vedere legal, terorismul informațional poate fi reprezentat de utilizarea abuzivă a sistemelor informatice digitale, rețelelor sau a altor componente pentru un rezultat final care sprijină sau facilitează o acțiune sau campanie teroristă.

Următoarea încercare de împărțire a tipurilor de terorism informațional vizează mijioacele și obiectivele urmărite de acesta. Exista două metode generale prin care un terorist ar putea desfășura un atac informațional terorist: atunci când este vizată tehnologia informației, și / sau când tehnologia informației reprezintă mijlocul prin care se realizează o operație mai largă.

Prima metodă se referă la faptul că un terorist ar putea viza un sistem informatic în vederea sabotării, fie aceasta fizică sau electronică, așadar distrugând sau afectând chiar sistemul informatic și orice infrastructură informațională (de exemplu, surse de energie electrică, comunicații etc.) în funcție de tehnologia vizată.

Cea de a doua metodă se referă la faptul că un terorist ar putea manipula și exploata un sistem informatic, prin alterarea sau furtul de date sau prin forțarea sistemului pentru îndeplinirea de către acesta a unor funcții pentru care acesta nu a fost destinat (de exemplu, utilizarea ilegală a unor mijloace de control aerian).

Pentru o mai bună înțelegere a conceptelor terorismului informatic vom prezenta un studiu de caz (un scenariu) asupra unor evenimente legate de tensiunile declanșate de sârbii bosniaci pe fondul nemulțumirii provocate de tratamentul discriminatoriu al Statelor Unite și NATO față de sârbii bosniaci și croați.

Ca urmare a nemulțumirilor existente de partea sârbă s-a format un grup paramilitar de sârbi din Bosnia, Serbia și din alte părți, intitulat „Consiliul Sârb pentru Eliberarea Bosniei" (SCLiB), cu influență politică și militară printre oficialii sârbi din Bosnia și din Yugoslavia; de asemenea, Consiliul este format din studenți sârbi din Slovenia, Ungaria și Yugoslavia și a început să-și sporească efectivele o dată ce membrii săi au început să comunice și să se întâlnească prin intermediul Intemet-ului, utilizând criptarea mesajelor pentru a-și ascunde intențiile și interesele.

[Reiese de aici posibilitatea ca grupuri de indivizi să poată

comunica în condiții destul de sigure prin intermediul mesajelor criptate transmise prin poșta electronică.]

Principalul lor obiectiv este răzbunarea, pentru alungarea mâhnirii provocate de ocuparea teritoriilor de către croați, împotriva ajutorului oferit de „stăpânii lor americani" și pentru îndepărtarea prezenței NATO din zonă prin dramatizarea cauzei lor în fața cetățenilor întregii lumi, influențându-i pe aceștia și, astfel, guvenele statelor cărora le aparțin, pentru a cere NATO să părăsească zona.

A fost provocată ciocnirea a 2 avioane C-130, în accident pierind toți membrii echipajelor ambelor avioane. Imediat după reușita atentatului au fost anunțați prin telefonul celular organizatorii, aflați în Slovenia, care au lansat imediat un „comunicat electronic", asumându-și responsabilitatea incidentului și prezentându-și manifestul și revendicările. Era indicată adresa de accesare a site-ului lor Web care era ruiat de pe un computer din Amsterdam de către studenți sloveni, prin intermediul unui cont „anonymous" din Finlanda. Acest mesaj a fost trimis către fiecare organizație importantă de știri electronice și tipărite din lumea industrializată.

[Este un scenariu perfect plauzibil și potențial spre a fi aplicat într-o situație asemănătoare pe vreun aeroport din țară, dacă ar exista o grupare locală suficient de bine înzestrată financiar și logistic și suficient de motivată pentru atingerea unui asemenea scop].

Conținutul acestei pagini de Web era dramatic și plin de elemente de propagandă și revendicări împotriva americanilor, a NATO și a atrocităților și imperialismului croat în regiunea balcanică și conținea afirmații nefondate asupra unor transferuri ilegale de arme între organisme ale NATO și croații sau musulmanii bosniaci. Au fost introduse câteva referințe asupra prezenței anterioare a americanilor în Liban și asupra modului în care a fost rezolvată această prezență.

Publicitatea rezultată este uluitoare: CNN, Reuters, ITAR-TASS și AP au difuzat imediat mesajul împreună eu adresa Web. La șase minute dupa primirea comunicatului electronic pagina de Web a

Consiliului a fost apelată pentru prima dată. La 24 de ore după atentat, pagina de Web a Consiliului primise peste un milion de apeluri.

[Transmiterea simultană a „comunicatului" prin intermediul poștei electronice la principalele agenții de presă a contribuit decisiv la amploarea publicității create în jurul atentatului]

La 24 de ore după prima accesare, primul sistem de pe care s-a realizat accesul a „crăpat", iar toate fișierele au fost șterse fără vreo posibilitate de recuperare, ca rezultat a unui program care se activa după 24 de ore, pe care hackerii Consiliului l-au inclus în conținutul paginii Web accesate, exploatând anumite defecte din limbajele de programare.

Deși acesta a creat un climat senzațional de teamă în întreaga lume a utilizatorilor obișnuiți de computere, cea mai mare pagubă a fost produsă organizațiilor de investigații și acelora ale apărării care au accesat imediat și, în mod natural, pagina de Web înainte ca organizațiile de știri să o răspândească. Printre aceste organizații s-au numărat Departamentul American al Apărării, ministerele apărării ale tuturor țărilor membre NATO, Departamentul Justiției, Departamentul Finanțelor și Agenția Centrală de Informații. Pagubele finale produse sistemelor nesecrete a fost incalculabil, dar dramatizarea cauzei Consiliului a fost cu adevărat eficientă.

[Este interesantă intenția teroriștilor de a spori interesul asupra evenimentului și de a întări impresia publicului asupra ineficienței acțiunilor autorităților prin distrugerea datelor conținute pe calculatoarele care au accesat pagina de Web, prin aceasta reușind să accentueze tensiunea provocată de atentat.]

Rapoartele asupra atentatului au ajuns la public împreună cu teama creată de dezastrele produse asupra computerelor și frustrarea generală asupra eforturilor americane în Balcani, creând o presiune enormă asupra Congresului și a Președintelui. Cu alegeri pentru Congres abia peste o lună, incidentul a devenit un punct de concentrare a presiunii congresmenilor asupra Președintelui, care a cedat în cele din urmă, în fața cererilor publicului și Congresului de aducere acasă a trupelor americane.

[Organizarea atentatului a fost destul de minuțioasă, având în vedere obținerea rezultatelor scontate, precum și asigurarea

integrității făptuitorilor prin studierea legislației celor două state, Olanda și Finlanda. Trebuie scoasă în evidență lipsa legislației române în cazul unor astfel de infracțiuni.]

Datorită lipsei unui tratat, agențiilor americane de investigații nu le-a fost permis să violeze protocoalele „cyber-comunității" finlandeze; așadar, investigatorii nu au putut să stabilească identitatea clientului serverului anonymous sau să localizeze poziția site-ului Web din Amsterdam. Teroriștii informatici ai Consiliului au rămas în anonimitate în siguranță, iar succesul lor în a se ascunde a determinat apariția mai multor pagini Web, „clone" ale celei originale a teroriștilor, apariția unei multitudini de „eliberatori ai Internet-ului" și recircularea manifestului original al Consiliului și a altor detalii prezente în pagina de Web a acestora.

[Teroriștii și-au atins cu claritate și eficiență obiectivul strategic.]

Se pune acum problema posibilităților de răspuns ale autorităților, plecând de la premisa că într-o societate democratică o dilemă în combaterea terorismului este reprezentată de găsirea unei echilibrări corecte între asigurarea drepturilor și a securității civile. Operațiunile militare într-o societate democratică, chiar dacă sunt destinate „protecției" acesteia, sunt adesea în discordanță cu principiile acelei societăți. Militarii se confruntă cu un paradox: deși teroriștii pot folosi forța brutală, nediscriminatorie față de civili sau militari, răspunsul militar trebuie să fie limitat și numai dacă făptuitorul unui act terorist este găsit ca fiind sponsorizat de către un anumit stat, este posibil un răspuns militar împotriva statului respectiv.

Guvernul Statelor Unite s-a lovit de un asemenea paradox cu ocazia confruntării cu terorismul informațional. Bazele de date, sistemele de computere, infrastructurile informatice militare, comerciale și civile în totalitate reprezintă obiective potențiale ale teroriștilor informaționali. Indiferent dacă prin intermediul unor mijioace fizice sau digitale, teroriștii informaționali pot distruge, afecta, degrada, interzice sau întârzia accesul la informațiile vitale pe care se bazează militarii și, astfel, putând deveni o amenințare în timp de pace, la fel de bine ca și pe timpul războiului.

[Se atrage atenția asupra dificultăților ivite atunci când trebuie răspuns unor asemenea acte teroriste și asupra nivelului amenințării prezentate de astfel de atacuri.]

Întotdeauna militarii vor constitui ținta teroriștilor informaționali. Mai mult, atacurile teroriștilor informaționali pot fi sponsorizate de un anumit stat și pot reprezenta prima undă a unui „Pearl Harbour digital". Originea atacurilor digitale este, în general, dificil de descoperit încă de la primul dintre acestea și în cazul în care atacul este într-adevăr, un precursor al unui război informațional dintre două state va fi necesar un răspuns militar.

Așadar, societățile democratice trebuie să evalueze cu grijă utilizarea forțelor militare pentru prevenirea și contracararea terorismului, chiar și în cazul în care militarii lor pot constitui ținta acestor atacuri. Prin determinarea militarilor să ofere un răspuns la acțiunile teroriste convenționale, teroriștii și cauza acestora pot căpăta un anumit grad de legitimitate. Ulterior acțiunile teroriste pot fi escaladate de la un nivel criminal la acela de „inamic al statului". Acest impas poate fi eliminat atunci când se iau contramăsuri teroriste.

[Se sugerează ca răspunsurile date unor asemenea atacuri să fie „anonime", rapide și pe deplin corelate cu potențialul atacatorilor. Se recomandă alcătuirea unor echipe mixte, formate din militari și din membri ai organizațiilor de supraveghere a respectării legilor. Din punctul de vedere al atribuțiilor, o astfel de structură poate să conțină militari cu un rol consultativ în cazul incidentelor obișnuite și, spre deosebire de acest caz, elemente de la agențiile de supraveghere a respectării legilor cu un rol consultativ în cazul unor incidente externe.]

Tehnicile ofensive de război informațional dezvoltate spre a fi utilizate de către militari la nivel de stat pot fi utilizate, de asemenea, pentru a răspunde terorismului informațional. În general, agențiile de supraveghere a respectării legilor nu dispun de posibilități asemănătoare pentru ducerea unui război informațional.

[Se prezintă necesitatea existenței unui grup specializat și integrat pentru a lupta împotriva terorismului informațional. Astfel de „Echipe de Răspuns Digital Integrat" vor lucra de la sisteme informatice conectate de la distanță și vor utiliza tactici de război informațional pentru a detecta, localiza și contracara teroriștii informaționali. Membrii acestora vor trebui organizați în celule

aflate la distanță, vor exploata elementele de resortul tehnologiei informațiilor, capacitățile de investigații și mijloacele de informații ale agențiilor de supraveghere a respectării legilor. Acești luptători informaționali, formați din membri de la mai multe arme (specialități), ca și din membri ai Departamentelor Justiției și Finanțelor vor lovi utilizând mijloace digitale computerele și rețelele utilizate de teroriștii informatici. Folosind un răspuns anonim, instituțiile guvernamentale pot lovi teroriștii informaționali fără a se afișa sau legitima, întrucât ambele pot conduce la răspunsuri fizice din partea acestora. Un astfel de răspuns oferă ultima dezmințire plauzibilă. Această structură ar putea combina elementele de investigații și cele jurisdicționale aparținând comunității care asigură respectarea legilor, cu posibilitățile ofensive ale militarilor.]

Posibilitățile noastre ofensive îndreptate împotriva unor competitori egali sau aproape egali sunt formidabile, indiferent dacă este cazul războiului informațional sau a celui convențional. Așadar, integrarea elementelor agențiilor de supraveghere a respectării legilor este necesară pentru a răspunde eficient la un atac dintr-o rețea dintr-o zonă gri.

[Este ilustrată astfel necesitatea existenței unei politici integrale, cu un răspuns pe deplin formulat, care să acopere spectrul amenințărilor bazate pe informații la adresa securității naționale, care să conducă elementele de ofensivă și apărare ce pot răspunde simetric și eficient.]

Deocamdată, România se găsește încă departe de riscurile unor asemenea amenințări, plecând, în special de la premisa inexistenței unei infrastructuri generale adecvate, dar asemenea amenințări pot ajuta mult la pregătirea unor măsuri de protecție pentru cazul în care vom *fi* în măsură să dispunem de ceva de apărat în acest domeniu. Mult mai aproape de realitate este problema supravegherii cetățenilor romani care, mai degrabă dezorganizat, sunt în măsură să realizeze atacuri asupra unor sisteme informatice din afara țării (acte considerate de legislația majorității statelor respective drept „terorism informațional") și, deci, mai în măsură să afecteze imaginea publică și interesele statului român.

Resurse URL (Uniform Resourse Locator)

Operații informaționale – în general
http://www.afcea.org și http://www.us.net/signal/
AFCEA publică regulat articole despre operațiile informaționale, intelligence și C2 în publicația lor lunară Signal.

http://www.aracnet.com/~gtr/archive/infowar.html
Bibliografia lui K. Anderson despre războiul informațional și documente despre vulnerabilitatea infrastructurilor.

http://huachuca-usaic.army.mil/
Centrul de Intelligence al Armatei SUA: publicații și doctrine.

http://www.aipio.asn.au/links.htm
Resurse URL australiene cu legături la multe resurse de intelligence din lume.

http://www.dodccrp.org/bostoc.htm
Lecții din Bosnia: Experiența IFOR (carte disponibilă electronic)

http://www.dodcerp.org
Programul de Cercetare Cooperativă C4ISR al Departamentului Apărării SUA și resursele Războiului Centrat pe Rețele

http://www.ndu.edu/inss/books/diw/index.html
Războiul Informațional Defensiv publicație a Universității Naționale a Apărării (NDU) a SUA

http://www.jya.com
Website actualizat zilnic cu articole internaționale și știri în domeniul criptografiei, războiului informațional, nivelul de comandă și intelligence-ului

http://www.rand.org/publications/MR/MR880/contents.html
In Athena's Camp: Pregătirea pentru conflict în Era Informațională. John Arquila și David Ronfeldt.

http://www.ndu.edu/inss/siws/cont.html
Sun Tuz, Arta Războiului în Războiul Informațional, carte electronică cu o colecție de articole.

http://www.infowar.com
Site-ul Winn Schwartau despre războiul informațional și securitate cu multe legături și articole.

http://www.infomatik.umu.se/~rhwit/IW.html
Paginile de război informațional ale lui Randy Whitaker de la Universitatea Suedeză Umea.

Resurse pentru operații informaționale
http://www.tno.nl/instit/fel/infoops
Resurse URL ale TNO-FEL despre Operații Informaționale, Siguranță Informațională, Securitate Informațională.

http://www.psycom.net/war.1.html
Institutul pentru studii avansate de război informațional (IASIW).

http://www.twurled-world.com/Infowar/Update2/cover.htm
Vedere de ansamblu a resurselor de război informațional din lumea întreagă bazată pe analiză de scanare web.

http://cryptome.org/fm100/fm100-6.htm
Manual de teren 100-6 : operații informaționale.
http://www.dtic.mil/doctrine/jel/cpubs2.htm
JS Join Publication 3-13: Doctrina Integrată pentru Operații Informaționale, 9 octombrie 1998; JS Join Publication 3-54: Doctrina Integrată pentru Operații de Securitate, 24 ianuarie 1997.

http://www.dtic.mil/doctrine/jv2020/jvpub.htm
JSJoin Vision 2020

Aspecte legale ale Operațiilor Informaționale
http://www.usdoj.gov/criminal/cybercrime
Departamentul de Justiție al SUA pentru Infracțiuni prin Calculator și Drepturi de Proprietate Intelectuală – articole și resurse.

http://www.dodccrp.org/iwilindex.htm
Război informațional și legi internaționale, L.T. Greenberg, S.E. Goodman, K.J. Soo Hoo, NDU.

http://www.cs.georgetown.edu/~denning/infosec/DOD-IO-legal.doc
Publicație amplă despre aspectele legale internaționale ale războiului informațional (Denning și Baugh, 1999).

http://www.leglnet.com/libr-inwa.htm
Biblioteca de legi pentru război informațional.

Siguranța informațională
http://www.cesg.gov.uk
Grupul pentru Securitate Comunicații – Electronică din UK.

http://www.itd.nrl.navy.mil/ITD/5540/main.html
Centrul Naval al SUA pentru Siguranța Înaltă a Sistemelor de Calcul – R&D

http://cve.mitre.org
Baza de date de vulnerabilități și expuneri uzuale, MITRE
http://www.robertgraham.com/pubs/network-intrusion-detection.html
Întrebări puse frecvent referitoare la sistemele de detecție a intruziunii pe rețele.

http://www-rnks.informatik.tu-cottbus.de/~sobirey/ids.html
Rezumat și legături la peste 80 de sisteme de detecție a intruziunii

http://www.clark.net/pub/roesch/public_html/secinfo.html
Lucrări și unelte de detecție a intruziunii, Martin Roesch.

http://jedefense.com
Jurnal de apărare electronică, articole orientate de Război Electronic.
http://niap.nist.gov/index.html
Parteneriatul de Siguranță Informațională Națională a SUA (NIST și NSA).

Infrastructura
http://www.aph.gov.au/library/pubs/rp/1997-98/rp18.htm
http://coombs.anu.edu.au/~acobb/X0016_Australias_Vulnerabi.html
http://www.infowar.com/CIVIL_DE/civil_100497a.html-ssi
Gândind la negândit: Vulnerabilități australiene la atacurile informaționale, Dr. Adam Cobb.

http://www.aracnet.com/~gtr/archive/index.html
Biografia lui Kent Anderson despre războiul informațional și documente de vulnerabilitate a infrastructurilor.

http://www.jwar.org
CIWARS: Jurnal de război infrastructural.
http://www.nipc.gov
NIPC: Centrul de Protecție a Infrastructurii Naționale a SUA.
http://www.pccip.gov
PCCIP: Comitetul Președințial al SUA pentru Protecția Infrastructurilor Critice – PDD 63 și raportul PCCIP.

Securitatea informației
http://www.cs.purdue.edu/coast/hotlist/
Arhiva COAST la Universitatea Purdue este probabil arhiva cea mai completă de legături referitoare la securitate de pe Internet.

http://www.tno.nl/fel/infosec
URL-ografie de securitate informațională menținută de TNO-FEL, un punct de start pentru multe resurse referitoare la securitatea informației.

Hacking

http://www.attrition.org/mirror/attrition
Site oglindă ce conține o arhivă la zi a site-urilor web stricate, paginilor lor stricate și a originalului lor.

http://www.ccc.de
CCC: Ggrupul de hackeri germani „Clubul de haos al calculatoarelor".

http://www.l0pht.com
Rezunat L0PHT de hacking, unelte și articole.

http://www.tno.nl/instit/fel/infosec
Resurse URL de hacking și intimidare menținute de TNO-FEL.

Răspuns la incidente și urgențe calculator

http://www.cert.org
Centrul de coordonare CERT : îndrumar de tratare a unui incident, rapoarte incident și recomandări.
http://ciac.llnl.gov/
CIAC: Departamentul Energiei al SUA, Capabilități de Recomandare pentru Incidente Calculator, buletine de securitate actualizate, unelte de securitate, informații despre anomalii și alte resurse de informații.

http://www.assist.mil/
DOD-CERT: Departamentul Apărării SUA, anunțuri și resurse informaționale ale echipei de răspuns la urgențe calculator.

http://www.first.org
FIRST: Forum de răspuns la incidente și echipe de securitate

http://www.telstra.com.au/info/security.html
TELSTRA: Index de referință australian pentru securitatea calculatoarelor și rețelelor.

DICȚIONAR

A

ACOPERIRE — acțiune militară prin care se face siguranța trupelor ce trec de la starea de pace la cea de război, se concentrează, realizează, dispozitive de luptă sau operative, ori se retrag.

ACOPERIREA FRONTIEREI DE STAT — operația executată în perioada inițială a războiului, de către grupări de forțe trecute în grabă la apărare pe frontiera de stat, cu scopul de a interzice o agresiune externă, a asigura desfășurarea oportună a mobilizării și realizarea dispozitivului strategic de apărare.

ACOPERIREA STRATEGICĂ — ansamblul de acțiuni militare realizate înainte, concomitent sau după declanșarea agresiunii cu rol de siguranță strategică, desfășurate simultan sau succesiv de către marile unități ale tuturor categoriilor de forțe ale armatei și celelalte forțe ale S.N.Ap. pe frontiera de stat și în adâncimea teritoriului, cu forțe gata de luptă permanent, pe baza unei concepții unitare, în scopul evitării surprinderii, opririi și respingerii agresiunii inamicului; în unele cazuri, pentru lichidarea capetelor de pod create de acesta la frontieră ori în adâncimea teritoriului național, asigurând condiții favorabile executării, mobilizării și desfășurării tuturor forțelor participante la război.

ACȚIUNEA DE LUPTĂ — acțiunea desfășurată de forțele armate aflate în conflinct, folosind armament și tehnică adecvate, cu scopul de a nimici, captura sau respinge acțiunile inamicului. Se desfășoară în mod organizat, folosindu-se forțe și mijloace de valoare variabilă și exprimă cel mai fidel trăsăturile caracteristice ale confruntării armate.

ACȚIUNE FLEXIBILĂ — o anume capcacitate a Forțelor Terestre de a-și adapta misiunile și modul de îndeplinire a acestora la o diversitate de scenarii de agresiune. Totodată acest principiu presupune o anumită abilitate în folosirea fiecărei arme (specialități), grupate pe module acționale, specifice misiunii și din perspectiva scopurilor planificate.

ACȚIUNE MILITARĂ — ansamblul măsurilor și activităților concepute, planificate și desfășurate de structurile militare pentru îndeplinirea

misiunilor încredințate, concretizate în formă de luptă armată, acțiuni nonviolente sau alte forme asociate acestora.

ACȚIUNE MILITARĂ ASOCIATĂ — acea acțiune prin care structurile militare sunt pregătite sau aduse în starea din care să poată desfășura acțiuni militare de luptă sau nonviolente.

ACȚIUNE MILITARĂ NONVIOLENTĂ — acea acțiune prin care o structură militară își pune în aplicare forța, de regulă, fără întrebuințarea armamentului.

ACȚIUNEA RAPIDĂ — exprimă necesitatea de a dispune marile unități și unitățile constituite în structuri mobile cu mare putere de foc și cu independență logistică, capabile de a riposta ferm și decisiv, în orice zonă (punct) de interes strategic.

ACȚIUNILE INTEGRATE — reprezintă un model de operaționalizare a zonei de operații și a teatrului de acțiuni militare de interes strategic, având ca notă dominantă acțiunea comună a tuturor/a majorității forțelor participante la acțiuni militare, în vederea atingerii unui scop comun.

ACȚIUNI SUBVERSIVE — formă de acțiune dusă cu mijloace ilegale, contrare normelor democratice specifice ordinii de drept, care vizează destabilizarea sistemului politic, dezorganizarea statului și a societății pentru a li se putea impune mai ușor condițiile care le lezează securitatea. Reprezintă o combinare a mijloacelor și metodelor teroriste cu cele proprii luptei politice, economice, psihologice sau de altă natură.

ACȚIUNI TERORISTE ȘI TERORIST-DIVERSIONISTE — agresiuni interne ilegale, imprevizibile, oculte, extrem de violente, ce se execută asupra unor obiective aparținând forțelor operaționale din raioanele acțiunilor de luptă, precum și asupra unor obiective politice, strategice, teritoriale, demografice, etnice, diplomatice din zona interioară a țării.

ADAPTABILITATE — capacitatea sistemului militar de a răspunde cu promptitudine la modificările apărute în înzestrare, organizare, concepte, proceduri și misiuni, fără diminuarea caracterului planificat și organizat.

ADÂNCIME — dimensiune spațială, măsurată de la linia frontului spre spatele acestuia, în limitele căruia sunt realizare dispozitivele subunităților, unităților și marilor unități destinate să îndeplinească o misiune de luptă atât în ofensivă cât și în apărare.

ADÂNCIMEA MISIUNII	adâncimea spațială din dispozitivul inamicului ce urmează să fie cucerită și care se stabilește prin conținutul misiuniii. Se măsoară de la limita dinainte a apărării inamicului și până la un aliniament situat în interiorul sau înapoia obiectivului ce urmează să fie cucerit.
AGILITATE	ușurință în mișcări; suplețe, sprinteneală, vioiciune.
AGRESIUNE	atac împotriva unei persoane sau a unui stat.
AGRESIUNE ARMATĂ	folosirea forței armate de către un stat împotriva suveranității, integrității teritoriale sau independenței politice a unui stat în orice mod incompatibil cu Carta Națiunilor Unite.
ALIANȚĂ MILITARĂ	înțelegere înscrisa într-un tratat prin care statele semnatare își asumă obligația reciprocă de a acționa cu toate sau numai cu o parte din forțele lor armate împotriva unui adversar comun.
AMENAJAREA GENISTICĂ	totalitatea lucrărilor genistice de fortificație, baraje, distrugeri, drumuri, poduri, treceri, mascare, asigurare cu apă și de adaptare a localităților, zonelor puternic industrializate, obiectivelor economice importante, obstacolelor și acoperirilor terenului din fâșia (zona) de acțiune a marii unități strategice (operative, tactice), executate într-o concepție unitară, în scopul interzicerii, îngreunării sau reducerii efectelor acțiunilor inamicului (adversarului) și asigurării condițiilor favorabile acțiunilor trupelor proprii.
AMENINȚARE CU FORȚA	săvârșirea de către un stat sau mai multe state a unor acte politice, economice, militare sau de altă natură, cu scopul de a impune altui stat să renunțe la deplina exercitare a drepturilor și atributelor suverane. Este o acțiune contrară principiilor și normelor de raporturi între state.
ANGAJARE	1. situație în care trupele se găsesc în contact cu inamicul și desfășoară acțiuni de luptă; 2. introducerea în luptă a unor forțe.
APĂRAREA	forma de luptă armată prin care se realizează respingerea, oprirea sau întârzierea acțiunilor inamicului, în scopul menținerii spațiului (terestru, aerian, maritim, fluvial) sau obiectivului încredințat.
APĂRAREA ACTIVĂ	capcacitatea sistemului defensiv de a lovi inamicul, în toate situațiile, prin foc la distanță mare, prin riposte ofensive violente sau prin procedee de acțiune ofensive,

dirijate asupra părților vulnerabile ale dispozitivului advers.

APĂRAREA ARMATĂ A ȚĂRII — ansamblul măsurilor și acțiunilor militare desfășurate unitar de Sistemul Național de Apărare în spațiul terestru, aerian și maritim (fluvial) în scopul descurajării, zădărnicirii și respingerii oricărei acțiuni militare care ar leza interesele fundamentale ale ROMÂNIEI.

APĂRAREA FLEXIBILĂ — adaptabilitatea promptă a Sistemului Național de Apărare la orice context întrevăzut în prognoza strategică precum și asigurarea posibilităților de a îmbina acțiunile de menținere fermă a celor mai importante raioane, obiective și aliniamente cu riposte ofensive ce vizează scopuri decisive.

APĂRAREA ÎN ÎNCERCUIRE — procedeul prin care forțele mențin o suprafață de teren (zonă, obiectiv), luptând cu un inamic care este dispus în jurul lor și acționează pe toate direcțiile.

APĂRAREA MOBILĂ — formă de ducere a luptei care se bazează pe folosirea unor acțiuni combinate, ofensive și de apărare, întârzietoare, în scopul canalizării acțiunilor inamicului pe o direcție care să ofere apărătorului condiții avantajoase pentru executarea ripostelor ofensive în flancuri și spatele inamicului, și care, în final, să ducă la încercuirea și nimicirea grupării principale de forțe, la refacerea dispozitivului pe aliniamentul inițial, iar pe direcțiile pe care înainteaza cu succes, chiar la generalizarea atitudinii ofensive.

APĂRAREA NAȚIONALĂ — totalitatea măsurilor și acțiunilor adoptate și desfășurate de autoritățile constituționale ale statului român în scopul garantării suveranității naționale, independenței și unității statului, integrității teritoriale a țării și a democrației constituționale.

APĂRAREA N.B.C. — ansamblul de măsuri și acțiuni ce se desfășoară în scopul menținerii capacității de luptă a trupelor în condițiile contaminării radioactive, biologice și chimice. Aceasta se realizează prin: evaluarea posibilităților și cunoașterea intențiilor inamicului privind întrebuințarea armelor de nimicire în masă; determinarea efectelor și urmărilor în cazul folosirii acestora; stabilirea măsurilor de protecție specifice și executarea decontaminării trupelor și terenului.

APĂRAREA PREGĂTITĂ DIN TIMP — procedeu defensiv care permite forțelor angajate în luptă să-și pună în aplicare, în volum complet elementele puterii de luptă.

APĂRAREA PREGĂTITĂ ÎN GRABĂ — procedeu defensiv care permite forțelor angajate în luptă să-și pună în aplicare, în volum redus, elementele puterii de luptă.

APĂRAREA ZONALĂ — formă particulară a operației de apărare ce se adoptă în plan local, în care forțele dintr-o anumită zonă acționează întrunit, după o concepție unitară, pentru respingerea ofensivei inamicului și nimicirea acestuia.

ARTA MILITARĂ — componentă a științei militare care are ca obiect de studiu teoria și practica organizării și ducerii luptei armate, a războiului în ansamblu. Studiază experiența luptei armate, elaborând principii, reguli, norme, procedee și metode de pregătire și ducere a acțiunilor militare în timp de război.

ASIGURAREA ACȚIUNILOR ȘI PROTECȚIA TRUPELOR — ansamblul de măsuri și acțiuni, desfășurare continuu într-o concepție unitară, de către toate forțele participante și la toate eșaloanele, destinate obținerii datelor necesare și creării condițiilor de securitate a personalului, tehnicii și sistemelor împotriva acțiuniii agresorului și a altor factori perturbatori, executate în scopul menținerii capacității de luptă a trupelor și îndeplinirii misiunilor primite.

ASIGURAREA CĂILOR DE COMUNICAȚIE — ansamblul de măsuri și acțiuni ce se întreprind pentru: alegerea, recunoașterea și pregătirea căilor de comunicații; repararea, restabilirea, întreținerea, paza și menținerea în stare de viabilitate a dumurilor, căilor ferate, gărilor, porturilor, aeroporturilor și lucrărilor de artă; organizarea și executarea serviciului de comenduire și îndrumare a circulației; cercetarea nucleară, biologică și chimică pe căile de comunicații, paza și apărarea lucrărilor de artă de pe acestea.

ASIGURAREA FINANCIARĂ — totalitatea măsurilor ce se iau în scopul stabilirii, cererii, obținerii, utilizării și justificării mijloacelor financiare destinate forțelor armate, pentru a le aproviziona la timp și fără întrerupere cu tehnică și materiale, precum și pentru plata drepturilor bănești cuvenite personalului.

ASIGURAREA MEDICALĂ — totalitatea măsurilor ce se iau în vederea păstrării sănătății militarilor, prevenirii apariției și răspândirii bolilor, acordării la timp a ajutorului medical, evacuării răniților și bolnavilor și spitalizării, tratamentului și recuperării acestora în scopul înapoierii în cel mai scurt timp la unități.

ASIGURAREA SANITAR- — menținerea sănătății a animalelor și prevenirea transmiterii bolilor de la animale la om, tratarea și

VETERINARĂ	evacuarea animalelor rănite și bolnave, cunoașterea stării epizootice din zonă, controlul sanitar-veterinar al alimentelor de origine animală, protecția sanitar-veterinară împotriva efectelor armelor de nimicire în masă, aprovizionarea forțelor cu animale pentru serviciu.
ASIGURAREA TEHNICĂ	ansamblul de măsuri, activități și operațiuni care se planifică, organizează și execută în scopul menținerii în permanență a unui înalt grad de completare cu tehnică militară și unei stări tehnice și de întreținere bună a acesteia, precum și a evacuării tehnicii deteriorate de pe câmpul de luptă.
ASISTENȚĂ JURIDICĂ	totalitatea măsurilor și acțiunilor întreprinse pentru a se asigura respectarea în acțiunile militare a cerințelor legilor țării, regulamentelor militare și ale dreptului internațional aplicabil în conflictele armate.
ASISTENȚĂ MUTUALĂ	înțelegere politico-militară între două sau mai multe state pentru apărarea comună împotriva unui atac armat.
ASISTENȚĂ NAȚIONALĂ	asistența militară sau civilă acordată de o forță străină unei națiuni prin intervenția pe teritoriul țării respective, pe timp de pace, în situații de criză sau război, în baza unor acorduri încheiate pe bază de reciprocitate.
ASISTENȚĂ UMANITARĂ	acțiuni desfășurate pentru înlăturarea efectelor dezastrelor naturale sau provocate de om, fiind limitate ca sop și durată, ele suplimentând sau completând eforturile depuse de națiunea în cauză.
ATITUDINE MENTALĂ " PREVENTIVĂ"	anticiparea posibilelor amenințări și a situațiilor de risc; vizează singerea „din față" a unor focare de conflict, a căror extindere, scăpând de sub control, ar putea aduce atingerea intereselor naționale ale României.
ATITUDINE MENTALĂ " REACTIVĂ"	orientarea spre înfrângerea ulterioară a unui inamic evident și cunoscut în toate componentele sale.
ATRIBUT (AL CONDUCERII)	o activitate, o obligație de a îndeplinii anumite sarcini sau operații ce se pot încredinta unui organ de conducere, compartiment sau persoană și care este dimensionat de structura sistemului și factorii care îl influențează.
AUTORITATE ASUMATĂ LEGAL	dreptul de a da ordine pe care un militar și-l asumă potrivit actelor normative în vigoare, a ierarhizării gradelor, funcțiilor și a competențelor în domeniu.

B

BĂTĂLIE — confruntare cu rol decisiv, din cadrul operației, prin care se asigură obținerea succesului în îndeplinirea obiectivului (scopului) urmărit de aceasta.

BLOCADĂ — acțiune desfășurată de forțe externe pentru întreruperea căilor de legătură maritime, terestre, aeriane, fluviale, a fluxurilor vitale de surse energetice, materii prime și materiale strategice, necesare desfășurării normale a activităților obiectivelor economice de importanță vitală etc.

C

CALITATE — totalitatea însușirilor și laturilor esențiale în virtutea cărora un lucru este ceea ce este, deosebindu-se de celelalte lucruri.

CAMPANIA — totalitatea operațiilor și luptelor forțelor armate desfășurate într-o perioadă de timp caracteristică (an, anotimp) sau într-o zonă geografică distinctă, pe baza unei concepții unitare, în vederea îndepliniii unor obiective strategice.

CAPABILITATE — posibilitatea de a săvârși ceva, de a fi în stare să execute ceva.

CAPACITATE — ansamblul cunoștințelor, abilităților, însușirilor psihice și comportamentelor necesare agentului acțiunii militare pentru realizarea unor acțiuni determinate.

CAPACITATEA ACȚIONALĂ A STRUCTURILOR — capacitatea de reacție a armatei în situațiile care necesită intervenția sa.

CAPACITATE DEFENSIVĂ CREDIBILĂ — principiul de bază al organizării Forțelor Terestre în timp de pace, care presupune restructurarea acestora în scopul realizării unei structuri militare descurajante, active, mobile, robuste, flexibile și suficiente, capabilă să asigure opreaționalizarea unei forțe de reacție ample și eficiente.

CAPACITATE OPERAȚIONALĂ — posibilitatea unității de a desfășura acțiuni militare în conformitate cu scopul pentru care a fost creată.

CAPACITĂȚI SPECIALE — posibilitățile unei unități de a desfășura pe lângă acțiunile de bază pentru care a fost creată și acțiuni complementare (nucleare, biologice și chimice; război electronic; apărare antiaeriană; apărare antiblindate; supraveghere electronică etc.).

CARACTERUL INTERARME ȘI INTEROGATORII DE FORȚE	asigură instruirea comandamentelor și trupelor în condițiile reale și complexe ale câmpului modern de luptă când misiunile nu mai pot fi îndeplinite decât cu participarea în funcție de amploarea forțelor angajate, a tuturor armelor și categoriilor de forțe aflate la dispoziția eșalonului tactic, operativ sau strategic.
CARACTERUL PULSATORIU (AL CÂMPULUI DE LUPTĂ)	presupune desfășurarea acțiunilor militare într-un ritm viu, trepidant în spațiul de confruntare.
CARACTER TRIDIMENSIONAL (AL CÂMPULUI DE LUPTĂ)	spațiul de confruntare poate fi terestru, aerian și maritim (fluvial).
CAZAREA TRUPELOR ȘI ADĂPOSTIREA ANIMALELOR	totalitatea măsurilor și acțiunilor ce se execută în scopul: asigurării cu terenuri, construcții, instalații și aprovizionarea cu materiale specifice; exploatării, întreținerii și reparării construcțiilor și instalațiilor; cazării personalului și adăpostirii animalelor în clădiri, corturi, adăposturi, vehicule speciale etc.; prevenirii și stingerii incendiilor.
CÂMP DE LUPTĂ	spațiul în care se desfășoară acțiunile militare în confruntarea directă și nemijlocită dintre părțile beligerante.
CÂMP DE LUPTĂ CIBERNETIZAT	spațiul de confruntare definit prin următoarele elemente: multitudinea sistemelor automatizate de armament și roboți utilizați pe câmpul de luptă; condiții impuse de comprimarea timpului operativ; multifuncționalitatea forțelor luptătoare; conservarea forțelor umane prin folosirea lor masivă numai în situații de mare dinamism; compensarea limitelor fiziologice ale comandanților, luptătorilor și operatorilor prin utilizarea roboților pentru activități care cer eforturi și timp îndelungat, atenție deosebită, migală, precizie, sacrificiu etc.
CÂMP DE LUPTĂ INTEGRAT	spațiul terestru, aerian și - după caz- maritim sau fluvial în care se dispun și duc lupte integrate forțele și mijloacele marilor unități și unităților tactice de arme întrunite, și cele aparținând celorlalte categorii de forțe armate care sunt subordonate temporar sau cu care cooperează, în vederea îndeplinirii misiunilor.
CERCETARE OPERAȚIONALĂ	disciplină științifică ce cuprinde un ansamblu de principii, metode și mijloace destinate elaborării de metodele

matematice ale fenomenelor și proceselor studiate. Are ca obiectiv fundamnetarea cantitativă a hotărârilor, prin elaborarea variantelor și criteriilor decizionale, studiul consecințelor imediate și de perspectivă ale acestora, evaluarea diferiților factori de influență.

CIOCNIREA — angajarea inamicului de către forțele proprii în confruntarea militară. Se desfășoară în timp scurt și, de regulă, este dusă de eșalonul brigadă (similar) și de inferioarele acestuia. Are loc, de regulă, între elementele de siguranță ale forțelor adverse și se poate transforma sau nu în luptă.

COEZIUNEA — coeziunea este unitate. Aceasta este o calitate care leagă împreuna părțile componente, care furnizează rezistență (elasticitate) împotriva acțiunilor distructive și a dezorganizării. Micșorează vulnerabilitatea structurilor la înfrângere și împotriva efectelor loviturilor adverse.

COLABORARE MILITARĂ INTERNAȚIONALĂ — promovarea și apărearea intereselor naționale în relațiile cu partenerii de dialog pentru edificarea unei arhitecturi de securitate viabile, care să contribuie la întarirea încrederii și a transparenței relațiilor dintre Armata României și armatele altor țări.

COMANDA — ansamblul acțiunilor prin care organul de conducere își impune voința asupra organelor de execuție pentru a acționa în sensul dorit; a comanda semnifică punerea în aplicare a unor decizii, planuri sau programe concepute în prealabil în vederea realizării obiectivului/scopului propus.

COMANDAMENTUL COMBINAT — este format din personal provenit din armatele a două sau mai multe țări.

COMANDAMENTUL FORȚELOR TERESTRE — structură de comandă, de concepție și execuție ce răspunde de întrebuințarea forțelor și mijloacelor din subordine; se înființeaza la război și se subordonează ierarhic Marelui Cartier General.

COMANDAMENTUL ÎNTRUNIT — este format din personal provenit din două sau mai multe categorii de forțe ale armatei și are în principiu structura unui comandament obișnuit.

COMANDAMENTUL LOGISTIC AL FORȚELOR TERESTRE — structură de comandă, de concepție și execuție ce răspunde de organizarea, planificarea și întrebuintarea forțelor și mijloacelor de logistică din subordine; funcționează la pace, în situații de criză și război și se subordonează ierarhic Statului Major al Forțelor Terestre (Comandamentului Forțelor Terestre).

COMANDAMENTUL OPERAȚIONAL INTERARME	organism ce trebuie să aibă o structură care să permită planificarea operațiilor integrate, dar și conducerea și controlul specific al forțelor din subordine.
COMANDAMENTUL OPERAȚIONAL OPERATIV/ TACTIC	structura de comandă ce are în subordine nemijlocită forțele operaționale de nivel operativ/tactic.
COMBATEREA TERORISMULUI	totalitatea acțiunilor care includ antiterorismul (măsuri defensive luate pentru reducerea vulnerabilității în fața actelor de terorism) și contraterorismul (măsuri luate pentru a împiedica, intimida și reacționa la actele de terorism) desfășurate în scopul combaterii terorismului în toată gama amenințărilor pe care le implică.
COMPATIBILITATE	capacitate a două sau mai multe părți de a funcționa împreuna fără o interferență reciprocă.
COMPETENȚĂ	normă strategică a organizării și executării instrucției și educației militare, semnificând totalitatea capacităților cognitive, psihomorale și psihomotrice prin care agentul acțiunii militare acționează individual și/sau în grup, pentru a asigura fucționalitatea structurii militare din care face parte.
COMPETENȚĂ PROFESIONALĂ (A MANAGEMENTULUI INSTRUCȚIEI)	selecționarea celor mai competente cadre și încadrarea acestora pe funcțiile prevăzute în structurile care planifică, organizează și coordonează instrucția armatei.
COMPETITIVITATE	dorința fiecărui militar de a fi cel mai bun și de a se compara permanent cu ceilalți în spiritul concurenței.
COMPLEMENTARITATE	transferul cunoștințelor și formarea deprinderilor necesare „luptătorului universal" care poate folosi în mod real toate categoriile de armament individual și tehnica de luptă din înzestrarea subunității.
COOPERAREA	activitatea prin care se asigură coordonarea acțiunilor tuturor forțelor participante la luptă (operație) în timp, spațiu și pe misiuni, în scopul concentrării și însumarii eforturilor acestora pentru îndeplinirea unei misiuni de luptă comune.
COORDONAREA	activitatea de menținere, păstrare și perfecționare a stării de ordonare a sistemului conducător și a celui condus, precum și a tuturor relațiilor dintre ele.

COORDONAREA INSTRUCȚIEI — ansamblul proceselor prin care se sincronizează deciziile și acțiunile personalului sistemului de instrucție al armatei, în ceea ce privește dirijarea resurselor, astfel încât, acestea să fie disponibile la timpul necesar, în cantitatea și de calitatea stabilită, în scopul realizării obiectivelor propuse.

COORDONAREA INSTRUCȚIEI ARMATEI (FUNCȚIE) — sincronizarea acțiunilor structurilor care planifică și conduc procesul de instrucție în vederea realizării obiectivelor stabilite.

CONDUCEREA INSTRUCȚIEI — mulțimea acțiunilor întreprinse de manager în vederea aplicării deciziilor prin exercitarea atribuțiilor de comandă și control.

CONDUCEREA FORȚELOR TERESTRE — ca activitate, este un atribut al Comandamentului Forțelor Terestre, iar ca element component al sistemului de conducere al sistemului de conducere al armatei, este construit din structuri de comandă cu atribuții și responsabilități în conceperea, administrarea și armonizarea măsurilor și acțiunilor destinate apărării, pentru trupele din subordine.

CONDUCEREA OPERAȚIONALĂ — totalitatea activităților și măsurilor întreprinse de către organele de conducere în scopul organizării și desfășurării luptei armate.

CONTINUĂRI — moduri probabile de acțiune bazate pe rezultatele posibile ale secvențelor sau ale cursului unei acțiuni militare.

CONTINUITATE — faptul, însușirea de a fi continuu, starea a ce este continuu.

CONFLICT ARMAT — confruntarea între două sau mai multe state, folosind forța armată, care urmărește rezolvarea unor neînțelegeri sau diferende de interese, atunci când reglementarea pașnică nu a reușit să le rezolve.

CONTRALOVITURĂ — ripostă ofensivă desfășurată în spațiul operativ de către mari unități, cu scopul de a nimici gruparea principală de forțe a inamicului pătruns în fâșia de apărare a unei mari unități operative.

CONTRAPREGĂTIREA — acțiunea de lovire prin foc masat, executată prin surprindere, cu toate mijloacele la dispoziție, asupra obiectivelor și grupărilor principale de forțe ale agresorului pregătite pentru ofensivă.

CONTROLUL — activitatea de cunoaștere a relațiilor și a modului de

aplicare a actelor normative ce reglementează activitatea domeniului militar.

CONTROLUL ARMAMENTELOR — implică orice plan, aranjament sau proces bazat pe acorduri internaționale și guvernează oricare dintre aspectele privind numărul, tipurile și caracteristicile performanțelor sistemelor de armamente, forța numerică, organizarea, echiparea și dislocarea forțelor armate menținute de părți în scopul reducerii instabilității în mediul militar.

CONTROLUL SISTEMULUI DE INSTRUCȚIE — ansamblul activităților desfășurate de structurile sistemului în vederea verificării stadiului de pregătire la un moment dat în comparație cu oviectivele stabilite pentru s dr interveni a se elimina neajunsurile care împiedică realizarea programului de instrucție.

CORPUL DE ARMATĂ TERITORIAL — mare unitate operativă, destinată să îndeplinească misiuni de apărare zonală, mobilizare și instruire a rezerviștilor. Are în compunere mari unități (unități, subunități) de arme întrunite, de armă și de asigurare a acțiunilor de luptă.

CREDIBILITATE — capacitatea organismului militar de a induce pe plan intern și extern percepții și convingeri ferme cu privire la potențialul de care dispune, pentru a desfășura cu succes acțiuni armate.

CRIZĂ — manifestare a unor dificultăți (economice, politice, sociale etc.); perioadă de tensiune, de tulburare, de încercari (adesea decisive) care se manifestă în societate. Moment critic care intervine în evoluția vieții internaționale, a raporturilor dintre state, a unui sistem, regim sau guvern.

D

DEBARCARE — moment (etapă, fază) din acțiunea de desantare care cuprinde atingerea solului de către desantul aerian parașutat sau aerotransportat și lupta pentru ocuparea primelor raioane ale subunităților desantate.

DECIZIE — hotărâre luată în urma examinării unei probleme, a unei situații etc., soluție adoptată (dintre mai multe posibile); rezoluție.

DEGREVARE — acțiunea de a degreva (a scădea, a reduce sarcinile sau obligațiile impuse unei persoane fizice sau unei instituții) și rezultatul ei.

DEMONSTRAȚIE DE FORȚĂ — operațiune menită să demonstreze capacitatea militară a unei alianțe, a unui stat sau a unei grupări de trupe dislocate într-o anumită zonă, în încercarea de a dezamorsa o anumită situație.

DEPLASAREA — acțiunea prin care marile unități (unitățile și subunitățile) și grupările de forțe sunt dislocate dintr-un loc în altul.

DEPLASAREA COMBINATĂ — acțiunea prin care o structură militară se deplasează prin marș și prin transport.

DEPLASAREA TRUPELOR — acțiune desfășurată de trupe pentru mutarea dintr-un raion în altul, intrarea în luptă sau efectuarea unei manevre, cu păstrarea completă a capacității de luptă în vederea îndeplinirii unei misiuni.

DESANT AERIAN — grupe de forțe făcând parte din dispozitivul de luptă (operativ sau strategic), transportată pe calea aerului (cu avioane, elicoptere, planoare) și întrebuințată, de regulă, în raioane din adâncimea dispozitivului inamicului, prin debarcare sau paraşutare în scopul îndeplinirii unei misiuni de luptă. Forțele utilizate pot fi trupe de paraşutiști sau trupe de orice armă, antrenate pentru ducerea unor astfel de acțiuni.

DESCOPERIRE — acțiunea de a descoperi (a găsi un lucru căutat, necunoscut sau ascuns; a afla) și rezultaul ei; ceea ce a fost descoperit, aflat.

DESCURAJARE — concept al unor doctrine militare contemporane, potrivit căruia se urmărește a determina adversarul să renunțe la anumite scopuri, acțiuni, mijloace, de teama ripostei și a riscurilor pe care le-ar atrage folosirea acestora.

DESCURAJARE ACTIVĂ — constituirea și dezvolatarea permanentă a unor forțe convenționale care să reprezinte un factor descurajant potrivit pentru un potențial adversar.

DESCURAJATOR — care te face să-ți peirzi curajul; demoralizant; deprimant.

DESFĂȘURARE STRATEGICĂ — ansamblul de măsuri organizatorice și de planificare, precum și activitățile practice începute încă din timp de pace și continuate în perioada de tensiune în relațiile internaționale sau după declanșarea acțiunilor militare, pentru trecerea forțelor armate și a forțelor de protecție de la starea de pace la cea de război, rirdicându-le capacitatea de luptă în trepte (succesiv) sau direct prin mobilizare, deplasarea lor în siguranță, către frontiera de stat, crearea grupărilor de forțe și a dispozitivului

strategic de apărare preconizat, concomitent cu trecerea economiei naționale la producția de război.

DETENSIONARE — acțiunea de a detensiona (a elimina sau a reduce tensiunea) și rezultatul ei.

DEVANSARE — o acțiune de depășire a inamicului, în timp și spațiu, cu scopul de a-l surprinde și de a-i micșora șansele, de a opune rezistență organizată. Se realizează exploatând rapid condițiile favorabile manifestate într-un moment.

DEZORGANIZARE — acțiune prin care se urmărește perturbarea gravă a sitemului de conducere a trupelor inamicului și a comunicațiilor acestuia.

DIFEREND — deosebiri de păreri între două sau mai multe persoane, state etc.; neînțelegere, dezacord.

DIGITAL — care generează, măsoară, prelucrează, sau stochează semnale digitale.

DIGITALIZARE — acțiunea de transformare a semnalelor analogige în semnale digitale.

DIGITALIZAT — care a fost transformat în semnal digital.

DINAMIC — plin de mișcare, de acțiune, activ; care este în continuă (și intensă) mișcare, evoluție, care se desfășoară rapid.

DINAMISM — putere vitală, forță de acțiune, de mișcare.

DIPLOMAȚIE PREVENTIVĂ — acțiuni diplomatice întreprinse înaintea unei crize previzibile, pentru prevenirea și limitarea violențelor.

DISCONTINUITATE — lipsă de continuitate între mai multe elemente care se succed în timp sau în spațiu; intermitență.

DISPOZITIV DE LUPTĂ — dispozitiv constituit în vederea desfășurării acțiunilor de luptă, care materializează hotărârea comandantului privind modalitatea de întrebuințare a forțelor și mijloacelor pentru îndeplinirea misiunii.

DISPUNEREA AVANSATĂ A FORȚELOR — impune (în dimensiunea ei operativă și tactică) „prepoziționarea" unor forțe pe direcțiile strategice, operative și chiar tactice, care să constituie un nucleu (cu o prezență înaintată) mobil cu rolul de a prelua „șocul" primelor acțiuni militare desfășurate în forță.

DIVERSIUNE	1. acțiune desfășurată cu scopul de a-l induce în eroare pe inamic asupra direcției principale de atac (direcții/ lovituri principale) sau a zonei (raionului) în care se pregătesc anumite acțiuni de luptă. 2. acțiune executată de grupări specializate pe teritoriul părții adverse cu scopul de a slăbi capacitatea de rezistență și moralul populației și al militarilor, folosind procedee specifice (sabotaje, răspândirea de zvonuri, manifeste etc.).
DOCTRINĂ	totalitatea principiilor unui sistem politic, științific, religios, militar.
DOCTRINA DE INSTRUCȚIE A ARMATEI	ansamblul tezelor, principiilor, regulilor și normelor adoptate de organismul militar cu privire la instrucția Armatei României, astfel încât aceasta să-și poată îndeplini misiunile ce-i revin pe timp de pace, în situații de criză și la război, potrivit prevederilor Constituției României și legilor în vigoare.
DOCTRINA MILITARĂ	concepție unitară adoptată de stat cu privire la război, armată și apărarea țării, ansamblul principiilor, metodelor și procedeelor preconizate și aplicate în pregătirea forțelor armate, a populației și în ducerea războiului, în raport cu condițiile, interesele și posibilitățile specifice ale statului.
DOCTRINA OPERAȚIONALĂ A FORȚELOR TERESTRE	totalitatea principiilor, operațiunilor, metodelor, obiectivelor și direcțiilor de acțiune a Forțelor Terestre precum și concepția de organizare, înzestrare și întrebuințare a acestora pe timp de pace, în situații de criză și la război, pentru îndeplinirea misiunilor ce le revin potrivit prevederilor legilor țării și ale regulamentelor militare în vigoare.
DREPT INTERNAȚIONAL	totalitatea normelor de drept care reglementează raporturile dintre state.
DREPT INTERNAȚIONAL UMANITAR	parte a dreptului internațional care asigură securitatea persoanelor civile, militarilor răniți sau bolnavilor, personalului medical și forțelor de protecție civilă în caz de conflict armat și a populației de pe teritoriile ocupate.
DURATA CICLULUI CONDUCERII	timpul necesar pentru exercitarea actului de comandă din momentul primirii misiunii sau informațiilor despre modificări esențiale ale situației până când eșalonul condus este capabil să desfășoare acțiuni în concordanță cu decizia comandantului.

E

ECHIPĂ — grup de oameni (militari) care, sub conducerea unui șef, îndeplinesc/execută în același timp o muncă/misiune sau o acțiune comună.

ECONOMIA DE FORȚE ȘI MIJLOACE — stabilirea, distribuirea și utilizarea judicioasă a posibilităților de luptă proprii, în raport cu necesitățile impuse de obiectiv și de obținerea de rezultate maxime cu eforturi, forțe, mijloace și pierderi minime.

EFICACITATE — măsura în care o activitate satisface o necesitate, realizează un obiectiv, îndeplinește o funcție; poate fi pozitivă, nulă sau negativă.

EFICIENȚĂ — raportul dintre eficacitate și costuri.

EFICIENȚA MANAGEMENTULUI INSTRUCȚIEI ARMATEI — gestionarea judicioasă a resurselor materiale și financiare, puse la dispoziție pe o perioadă delimitată de timp, astfel încât cu resurse minime să se obțină rezultate maxime.

EFORT DE APĂRARE — totalitatea eforturilor materiale, umane, culturale, pe care un stat le face pentru apărarea proprie sau a aliaților în cazul unei agresiuni.

ESTIMARE — activitate prin care un compartiment, în urma unui proces de analiză, emite concluzii și propuneri (necesitate; posibilitate; mod de rezolvare; cerințe operaționale, materiale, financiare) cu privire la o situație, misiune sau ordin.

F

FLEXIBILITATEA ACȚIUNILOR MILITARE — exprimă o caracteristică a conducerii care se răsfrânge asupra elasticității și supleței execuției și desemnează capacitatea comandamentelor de a prevedea evoluțiile ulterioare, precum și de a adapta rapid atât ele cât și trupele, la schimbările dese și neașteptate care au loc pe câmpul de luptă.

FLEXIBILITATEA INSTRUCȚIEI MILITARE — capacitatea sistemului de instrucție de a permite extinderea/diminuarea unor activități, schimbarea/redimensionarea obiectivelor în funcție de prioritățile impuse.

FLEXIBILITATEA — adoptarea formelor optime de organizare, funcție de

MANAGEMENTULUI INSTRUCȚIEI	schimbările survenite în sistemul militar NATO, în strânsă concordanță cu influențele pe care le oferă resursele umane, materiale și financiare avute la dispoziție.
FOLOSIREA EFICIENTĂ A RESURSELOR	corelarea strictă a obiectivelor cu resursele avute la dispoziție astfel încât, pentru fiecare obiectiv de instrucție să se consume numai cât este necesar.
FORȚE DE ANGAJARE IMEDIATĂ (F.A.I.)	mari unități (unități) de armă și specialități, dispuse pe limita dinainte a dispozitivului și întrebuințate pentru producerea de pierderi cât mai mari agresorului, slăbirea capacității de luptă și oprirea ofensivei acestuia, limitarea pătrunderii în adâncimea apărării, menținerea zonelor (fâșiilor, raioanelor) încredințate și crearea condițiilor necesare trecerii la ofensivă.
FORȚE DE ANGAJARE ULTERIOARĂ (F.A.U.)	acele forțe dispuse în adâncimea dispozitivului în scopul executării ripostelor ofensive, apărării unor raioane (aliniamente) din adâncime, nimicirii desantului aerian (maritim) și trupelor aeromobile, înlocuirii unor grupări din forțele de angajare imediată care au suferit pierderi mari și închiderii unor breșe din dispozitiv apărute ca urmare a întrebuințării de către agresor a armelor N.B.C.
FORȚE DE SPRIJIN (F.S.)	forțe destinate să susțină forțele angajate pentru îndeplinirea scopurilor operației. Ele cuprind, de regulă, mari unități (unități, subunități) de artilerie și rachete, artilerie antitanc, aviație de sprijin, artilerie și rachete antiaeriene, cercetare, război electronic, radiolocație, geniu, protecție N.B.C., mijloace incendiare și furnizare.
FORȚE TERESTRE (F.T.)	principala categorie de forțe destinate să desfășoare acțiuni militare întrunite, independent sau în comun cu celelalte forțe, pentru apărarea armată a țării, în orice zonă de operații, condiții de climă și relief și reprezintă forța întrunită, capabilă să realizeze prezența, extinderea, continuitatea și dominația în teren și să susțină în orice moment toată gama acțiunilor militare necesare îndeplinirii scopului propus. Ele au capacitatea de a se proiecta rapid, generând forțe care să răspundă cerințelor în situații de criză, cât și forțe redimensionate pentru starea de război, prin mobilizarea resurselor puse la dispoziție.
FORȚE TERESTRE DE REACȚIE ÎN SITUAȚII DE	acele forțe destinate intervenției pentru gestionarea situațiilor de criză care pun în pericol interesele naționale fundamentale, asigurării îndeplinirii angajamentelor militare internaționale asumate de România, participării

CRIZĂ (F.T.R.S.C.)	la prevenirea, limitarea și înlaturarea urmărilor unor dezastre.
FORȚE TERESTRE DE REACȚIE RAPIDĂ (F.T.R.R.)	grupare de forțe constituită din mari unități și unități mecanizate, de tancuri, vânători de munte, parașutiști și poliție militară, înzestrate cu armament nou, destinate să asigure prima ripostă în situație de criză și conflict, să participe pe timp de război la îndeplinirea obiectivelor apărării armate a țării și să fie întrebuințată în cadrul structurilor multinaționale în operații militare altele decât războiul.
FORȚE TERESTRE DE REZERVĂ (F.T.R.)	centrele de mobilizare (I., Tc., Art.At., Art.AA., Ge., Po., Nv.Tp.Flv., Pșt. N.B.C., Cc., Trs.) destinate pentru realizarea capacității de acțiune la război.
FORȚE TERESTRE DE SPRIJIN (F.T.S.)	grupare de forțe constituită din mari unități și unități de artilerie, artilerie antitanc, artilerie antiaeriană, geniu, apărare N.B.C., transmisiuni și acțiuni psihologice, destinată pentru sprijinul Forțelor Terestre de Reacție Rapidă.
FORȚE TERESTRE DE SUPRAVEGHERE ȘI AVERTIZARE TIMPURIE (F.S.A.T.)	unități, subunități și formațiuni de cercetare, război electronic și cercetare radio, radiolocație, transmisiuni, control N.B.C și acțiuni psihologice, destinate pentru descpoerirea, identificarea, localizarea și determinarea momentului de acțiune a factorilor de risc la adresa apărării naționale.
FORȚE TERESTRE PRINCIPALE (F.T.P.)	centrele de instrucție și mobilizare (Mc., Tc., V.M., Art., Art.A.T., Trs.) destinate pentru amplificarea capacității de reacție a Forțelor Terestre în situații de criză sau război, asigurarea condițiilor pentru executarea mobilizării și constituirea forțelor de rezervă.

G

GESTIONAREA UNEI CRIZE	ansamblul măsurilor și acțiunilor de izolare - blocare a conflictelor care alimentează criza (conflictul).
GRUPAREA DE ANGAJARE	elementul principal al dispozitivului, destinat pentru îndeplinirea scopurilor operației prin producerea de pierderi cât mai mari, slăbirea treptată a capacității de luptă a grupărilor de forțe ale inamicului, oprirea ofensivei acestora și crearea condițiilor necesare pentru trecerea la ofensivă.
GRUPAREA DE	se constituie din mari unități de arme întrunite din forțele de angajare ulterioară, mari unități regrupate de pe

CONTRALOVITURĂ (CONTRAATAC) direcțiile unde agresorul nu acționează cu forțe puternice și, în situații deosebite, din rezervă. Valoarea forțelor pentru contralovitură trebuie să asigure superioritatea pe direcția ripostei ofensive și succesul acesteia.

GRUPARE INTERARME un sistem de forțe de natură și de volum foarte diverse, constituit temporar sau pemanent în cadrul unei categorii distincte de forțe ale armatei în vederea îndeplinirii unei misiuni comune.

GRUPARE OPERAȚIONALĂ acea grupare de forțe și mijloace, precum și posibilitățile de foc și mișcare ale acesteia, care este destinată îndeplinirii unei anumite misiuni, la un moment dat, în strânsă corelare cu situația creată.

I

IMAGOLOGIE ramură a sociopsihologiei care cercetează sistematic reprezentările pe care le au popoarele sau clasele sociale despre ele însele.

INSTRUCTOR cadru militar/militar angajat pe bază de contract/gradat, competent pentru a instrui un individ sau grup de indivizi din structurile armate.

INSTRUIREA PENTRU LUPTĂ A COMANDAMENTELOR/ COMEZILOR proces care constă în ridicarea nivelului de cunoștințe militare și de specialitate; perfecționarea deprinderilor necesare îndeplinirii atribuțiilor funcționale; închegarea acțiunii elementelor componente pentru a asigura funcționarea acestor tipuri de structuri în concordanță cu misiunile care le revin în situații de pace, de criză sau război.

INSTRUMENTELE mijloacele care ajută în mod intrinsec la realizarea în practică a unei tehnici, metode sau procedeu.

INSTRUCȚIA ARMATEI totalitatea activităților de pregătire a resursei umane pentru înzestrarea acesteia cu competențe, potrivit sarcinilor și responsabilităților funcționale care să o facă să acționeze eficient în structurile militare existente și din care face parte.

INSTRUCȚIA COLECTIVĂ forma de instrucție care se execută începând cu subunitatea de cel mai mic nivel, respectiv grupa, echipa/ similare, terminând cu unitatea și care are drept scop însușirea cunoștințelor și formarea deprinderilor necesare acțiunii întrunite a acestora, având două componente: una comună tuturor armelor și una specifică.

Este condusă de comandamentul nemijlocit al eșalonulu care se instruiește și se execută numai în perioad instrucției subunităților și unităților și numai de către acele structuri militare încadrate cu efective complete.

INSTRUCȚIA INDIVIDUALĂ — formă de instrucție care se execută în scopul însușiri cunoștințelor și formării deprinderilor generale de militar de luptător și specialist în armă, fiind condusă direct d comandantul nemijlocit, prin aplicarea metodelor d instruire specifice tehnicilor rapide de pregătir profesionalizată a trupelor.

INSTRUCȚIA INTEGRATĂ — forma de instrucție care asigură pregătirea subunităților unităților în vederea îndeplinirii misiunilor de luptă împreuna cu forțe și mijloace aparținând celorlalt structuri militare, arme sau categorii de forțe ale armate pe care le primește ca întărire, în sprijin sau cu car cooperează, în scopul realizării unității de conducere ș acțiune.

INSTRUCȚIA OPERAȚIONALĂ — forma de instrucție care vizează pregătirea subunităților unităților/formațiunilor, pentru îndeplinirea unor misiun specifice pe teritoriul național/în afara acestuia și s execută din momentul nominalizării acestora până la dat stabilită prin ordin să fie operaționale.

INSTRUCȚIA PENTRU LUPTĂ A ARMATEI — totalitatea activităților de instrucție a militarilor subunităților, unităților, marilor unități, comandamentelo și statelor majore, desfășurate în scopul însușiri cunoștințelor necesare pregătirii și ducerii luptei, formări deprinderilor de utilizare eficientă a tehnicii militare dir dotare și de conducere a structurilor militare din subordin pentru îndeplinirea misiunilor ce le revin la pace, în situații de criză sau la război. Instrucția pentru luptă a armatei mai cuprinde și latura teoretică și practică a pregătirii necesare acțiunilor nonviolente de tipu asimetric (armată contra grupuri neorganizate după tipologia militară) specifice situațiilor de pace și criză precum și formarea capabilităților acționale necesar intervenției la calamități și dezastre.

INSTRUCȚIA PENTRU OPERAȚII INTEGRATE MULTINAȚIONALE — forma de instrucție care se vizează pregătirea în comun a subunităților/unităților cu structuri similare aparținân armatelor statelor partenere, pentru îndeplinirea uno misiuni specifice de menținere a păcii, căutare-salvare umanitare.

INSTRUCȚIA SPECIALĂ A ARMEI — forma de instrucție care vizează pregătirea subunităților și unităților în vederea îndeplinirii misiunilor de luptă specifice fiecărei arme.

INTEGRALITATE — concertarea instrucției în scopul obținerii "luptătorului performant", abil mânuitor al mijloacelor de luptă, cu mentalitate de învingator, eficient în situații limită, capabil de autocontrol, adept al spiritului de echipă, cooperant și excelent camarad.

INTEROPERABILITATE — capacitatea comandamentelor și forțelor țărilor partenere de a acționa în comun cu cele ale țările membre NATO.

INTEROPERABILITATEA LOGISTICĂ — capacităților sistemelor unităților, subunităților și formațiunilor de logistică de a furniza servicii către și de a accepta servicii de la alte sisteme și forțe de logistică de același fel și de a utiliza serviciile astfel schimbate, pentru a le face capabile să opereze efectiv împreună.

L

LEGEA CONCORDANȚEI DINTRE SCOPURI, FORȚE ȘI MIJLOACE — obiectivele și misiunile trebuie astfel stabilite încât să corespundă posibilităților acționale ale forțelor și mijloacelor avute la dispoziție. Exigențele legii implică o analiză temeinică și multilaterală a situației, a cantității și mai ales a calității forțelor și mijloacelor de care se dipune pentru stabilirea, pe baze realiste, a grupărilor de forțe și mijloace necesare nimicirii inamicului.

LEGEA DEPENDENȚEI FORMELOR ȘI PROCEDEELOR ACȚIUNILOR MILITARE DE NIVELUL DEZVOLTĂRII ARMAMENTULUI ȘI TEHNICII DE LUPTĂ — exprimă necesitatea adoptării unor noi procedee și chiar forme de luptă care să corespundă caracteristicilor tehnico-tactice ale armamentului nou introdus în înzestrarea armatei și schimbărilor calitative ce apar în domeniul tehnicii de luptă.

LEGILE LUPTEI ARMATE — raporturi esențiale, obligatorii, generale, caracterizate prin repetabilitate și stabilitate relativă între componentele interne ale fenomenului militar, precum și între acestea și alte domenii sociale, care determină pregătirea și desfășurarea acțiunilor militare.

LEGEA RAPORTULUI DE FORȚE	condiționează obținerea succesului în lupta de realizare a unei superiorități de forțe și mijloace față de adversar în raioanele și pe direcțiile cele mai importante. În esență exprimă relația dintre cantitatea și calitatea forțelor și mijloacelor părților care se înfruntă prin luptă armată, relație exprimată cu un grad ridicat de probabilitate.
LEGEA UNITĂȚII ACȚIUNILOR	exprimă conexiunea luptei armate din toate mediile în care se desfășoară.
LIBERTATEA DE ACȚIUNE	asigurarea condițiilor de autonomie în decizie, planificarea și desfășurarea acțiunilor proprii și de limitare, pnă la anihilare, a posibilităților de opțiune și acțiune ale inamicului.
LOGISTICA	un complex de măsuri și acțiuni desfășurate pentru asigurarea condițiilor materiale necesare pregătirii și ducerii acțiunilor militare.
LOGISTICA FORȚELOR TERESTRE	un complex de măsuri și activități desfășurate pentru aprovizionarea forțelor destinate ducerii acțiunilor militare, transportul, mentenența, asigurarea medicală, sanitar-veterinară financiară a căilor de comunicație, cartiruirea trupelor și adăpostirea animalelor pentru îndeplinirea misiunilor ce-i revin acestor categorii de forțe ale armatei pe timp de pace, în situații de criză și la război.
LOGISTICA INSTRUCȚIEI	totalitatea activităților desfășurate de organele de specialitate și abilitate pentru asigurarea bazei materiale și tehnice necesare desfășurării instrucției, conform normelor de echipare, cazare, hrănire și dotare cu tehnică a structurilor în strânsă concordanță cu posibilitățile bugetare are Ministerului Apărării Naționale.
LOGISTICA TRUPELOR	totalitatea activităților ce se desfășoară în scopul asigurării marilor unități, unităților și subunităților cu tot ceea ce le este necesar pentru pregătirea și ducerea acțiunilor.
LOVITURA FRONTALĂ	constă dintr-o puternică pregătire de foc, după care trupele rup apărarea inamicului, pătrund în adâncimea dispozitivului acestuia executând concomitent manevre de învăluire pentru încercuirea și nimicirea pe părți a adversarului. Se execută pe una sau mai multe direcții, de regulă acolo unde apărarea inamicului este mai slabă.
LOVITURA ÎN ADÂNCIME	o formă de manevră în cadrul operației ofensive, care presupune constituirea unor puternice grupări de manevră capabile să pătrundă în adâncimea dispozitivului

inamicului în scopul lovirii decisive a obiectivelor importante de pe direcțiile de ofensivă, acționând concomitent cu forțele care lovesc frontal inamicul.

LOVIREA DE DIRECȚII CONVERGENTE — constă în acțiunea simultană a unor grupări de forțe separate, pe direcții care converg spre obiective importante din dispozitivul inamicului.

LUCRUL ÎN ECHIPĂ — presupune eforul operativ al membrilor unui grup pentru realizarea unor scopuri comune; încredere și confidențialitate; delegare de autoritate/competență și cooperare în cadrul echipei.

LUPTA — confruntarea armată sau un șir de confruntări prin care se urmărește îndeplinirea unor scopuri de importanță tactică.

LUPTA ARMATĂ — confruntarea militară violentă între două forțe adverse cu putere de luptă și care urmăresc, fiecare în parte, îndeplinirea scopurilor propuse.

LUPTA DE ÎNTÂLNIRE — procedeul prin care două grupări de forțe adverse, în mișcare din sensuri opuse, angajează lupta urmărind realizarea scopurilor propuse prin acțiuni ofensive.

LUPTĂTOR — persoană dotată fizic, intelectual, moral și psihic care poate duce acțiuni de luptă individuale sau în cadrul unui colectiv (structură militară) la cele mai înalte standarde.

M

MANAGENTUL CRIZEI — procesul de prevenire, limitare sau soluționare a crizelor. El stabilește procedurile și activitățile planificate și desfășurate pentru a aduce criza sub controlul celor care o gestionează, pentru a le permite acestora, ca prin acțiunile lor, să oprească evoluția ei următoare.

MANEVRA — ansamblul acțiunilor prin care se urmărește realizarea în ascuns a celei mai corespunzătoare grupări de forțe și mijloace în locul și la timpul stabilit și punerea lor într-o situație favorabilă pentru executarea unor loviturii hotărâtoare asupra inamicului sau pentru sustragerea forțelor proprii de sub loviturile acestuia.

MANEVRA DE ÎNTOARCERE — constă în fixarea și angajarea de front a inamicului cu o parte din forțe, iar cu gruparea principală acționându-se în flancul și spatele dispozitivului acestuia, pe o adâncime cât mai mare, cu interceptarea comunicațiilor pentru interzicerea acțiunilor forțelor inamicului care se retrag

	și ale rezervelor sale ce afluiesc din adâncime. Se adoptă în scopul nimicirii întregii grupări de forțe ale inamicului.
MANEVRA DE ÎNVALUIRE	constă în executarea unor lovituri care să conducă rapid în flancul și în spatele forțelor principale ale inamicului pătruns pe teritoriul național, alegându-se în general locurile cele mai slabe ale dispozitivului acestuia (intervale, flancuri, goluri), în scopul nimicirii lui pe părți într-un timp relativ scurt.
MANEVRA DE DIRECȚII INTERIOARE (DIN POZIȚIE CENTRALĂ)	o formă de manevră care se aplică pentru nimicirea succesivă sau pe părți a grupărilor inamicului. Se adoptă atât în ofensivă cât și în apărare, atunci când inamicul acționează cu mai multe grupări, iar forțele proprii se găsesc într-o poziție centrală și nu pot face față concomitent grupărilor acestuia.
MARȘUL	deplasarea organizată a structurilor militare pe vehicule proprii (tehnică blindată) sau pe jos (schi).
MASCAREA	ansamblul de măsuri și acțiuni care se planifică și se desfășoară pentru ascunderea elementelor dispozitivului și a activităților trupelor proprii față de concentrarea de toate categoriile a inamicului, precum și pentru inducerea în eroare a acestuia aupra situației, intențiilor, acțiunilor și posibilităților trupelor proprii în timp și spațiu.
MENTENANȚĂ	totalitatea măsurilor întreprinse pentru a menține sau a restabili starea de utilizare/funcționare a materialelor și a tehnicii la parametrii specifici, acestea incluzând inspectarea, tratarea, service-ul (întreținerea+reparațiile curente), stabilirea categoriei, reparațiile, refacerea, recondiționarea/modernizarea.
MENȚINEREA PĂCII	efortul de căutare a păcii de către părțile implicate și de către unii terți interesați, contribuind totodată la gestionarea unui conflict.
METODA CONDUCERII PRIN OBIECTIVE	determină rezolvarea simultană a unor pași, prin delegare de competență, concomitent cu creșterea eficacității elementului condus.
METODA INSTRUIRII ÎN PUNCTE DE BAZĂ	constă în realizarea transferului de cunoștințe prin parcurgerea etapei intuiției vii și pregătirii aperceptive sub conducerea directă și nemijlocită a instructorului în vederea inițierii și formării corecte a deprinderilor de bază ale luptătorului individual sau colectiv.

METODA PREGĂTIRII ÎN PUNCTELE PERMANENTE — constă în parcurgerea de către fiecare luptător în mod individual, prin procedeul autoinstruirii/descoperirii următoarelor etape psihopedagogice de învățare și instruire: însusirea teoretică și învățarea practică; recunoașterea și comparația; sintetizarea și reproducerea; uitarea și memorarea remanentă; execuția și corecția secvențială; exersarea și automatizarea; antrenamentul și perfecționarea, în scopul realizării transferului de cunoștințe, capabilități psiho-motrice și acționale necesare îndeplinirii misiunilor de luptă.

METODĂ DE CONDUCERE — modalitatea prin care conducătorul militar consideră că se poate îndeplini misiunea cu eficiență maximă. Viabilitatea acesteia se determină prin analiza raportului dintre obiectivul de îndeplinit și costurile obținute.

MODELUL — arhitectura ideală care integrează într-un tot unitar competențele cu care trebuie să fie înzestrat agentul acțiunii militare pentru a corespunde rolurilor și funcțiilor create în cadrul structurilor militare.

MORALUL (MILITARILOR) — ansamblul stărilor de spirit succesive ale militarilor în legătură cu îndeplinirea unor activități specifice armatei, având ca determinări obiective dimensiunile cadrului sociomaterial al activității militare (instrucție sau luptă), ca sursă psihologică.

MULTIDISCIPLINARITATEA — presupune formare și dezvoltarea luptătorului complet, cu un important grad de autonomie acțională în îndeplinirea misiunilor de luptă.

O

OBIECTIVELE INSTRUCȚIEI — finalitățile/ ceea ce urmează să fie realizat, către care este orientată întreaga activitate de instrucție.

OBIECTIVUL FUNDAMENTAL AL ÎNVATAMÂNTULUI MILITAR — formarea, specializarea și perfecționarea succesivă a cadrelor militare active și în rezervă ca profesioniști autentici, cetățeni culți, cu o aleasă educație patriotică, morală și civică, în spiritul tradițiilor omeniei și demnității, specialiști cu temeinice cunoștințe, priceperi și deprinderi în domeniile necesare Forțele Terestre, cu profunde convingeri și corecte atitudini față de valorile supreme ale statului de drept, capabile să-și îndeplinească atribuțiilor ce le revin la pace, în situații de criză și război.

OBIECTIVUL PRINCIPAL AL INSTRUCȚIEI — dezvoltarea capacității structurilor de comandă de a conduce acțiuni militare în situații complexe și realizarea unui nivel ridicat de instruire a structurilor acționale.

FORȚELOR TERESTRE	
OPERATIV	care lucrează repede, expeditiv, activ; termenul se asociază direct sau indirect unei acțiuni care este dorită să se desfășoare cât mai repede, cu o eficiență cât mai apropiată de scopul propus, deci cu rezultate finale favorabile.
OPERATIVITATE	calitatea de a fi operativ, calitate a conducerii trupelor concretizată în rapiditate și eficiență în reculegerea, prelucrarea și transmiterea informațiilor (ordinelor, dispozițiilor) necesare conducerii acțiunilor de luptă.
OPERAȚIA	ansamblul de acțiuni militare complexe, desfășurate unitar, în mediul terestru, aerian, maritim sau fluvial, prin care se urmărește îndeplinirea unor scopuri de importanță operativă sau strategică.
OPERAȚIA DE APĂRARE	ansamblul acțiunilor desfășurate de forțe întrunite cu rol strategic sau operativ, într-un spațiu geografic (fâșie, zonă), care include cel puțin o direcție de interes sau un obiectiv de menținut, prin care se asigură îndeplinirea unor scopuri parțiale ale operației de nivel strategic.
OPERAȚIA ÎNTRUNITA	totalitatea acțiunilor duse de o grupare de forțe cu rol strategic sau operativ, constituită din trupe aparținând mai multor categorii de forțe armate, sub comandă unică, în mediul corespunzător fiecăruia, dar cu un scop unitar.
OPERAȚIA OFENSIVĂ	ansamblul acțiunilor desfășurate de forțe cu rol strategic (operativ) într-un spațiu geografic (zonă, fâșie) ce include cel puțin o direcție sau un obiectiv, prin cucerirea cărora se realizează unul sau mai multe scopuri parțiale ale apărării armate a țării (operației de nivel strategic).
OPERAȚIA TERESTRĂ	acțiunea dusă de o grupare de forțe terestre cu rol operativ sau strategic, independent sau în cooperare cu grupări de forțe din celelalte categorii de forțe ale armatei, după un plan unic, cu scopul de a apăra sau cuceri obiective terestre de importanță operativă sau strategică.
OPERAȚII DE "ARĂTARE"/ EXPUNERE A FORȚEI	acțiuni destinate să demonstreze hotărârea României, implicând o activitate crescută a forțelor sale dislocate, în încercarea de a dezamorsa o situație specifică, care, dacă ar continua, ar periclita interesele sau obiectivele naționale.
OPERAȚII DE	operații desfășurate pentru căutarea, localizarea,

CĂUTARE-SALVARE (RECUPERARE)	identificarea, salvarea si recuperarea personalului, a echipamentului sensibil sau materialelor importante pentru securitatea națională.
OPERAȚII DE EVACUARE A NONCOMBATANȚILOR	acele acțiuni desfășurate pentru a evacua noncombatanții aflați sub amenințare, dintr-o țară străină. Aceste operații implică în mod normal cetățeni ai României sau a unei națiuni aliate, a căror viață este în pericol și pot implica totodată evacuarea selectivă a cetățenilor națiunii gazdă precum și cetățenilor altor țări.
OPERAȚII DE IMPUNERE A PĂCII	operații de folosire a forței militare sau de amenințare cu acesta, desfășurate în conformitate cu rezoluțiile și sancțiunilor destinate menținerii sau restabilirii păcii și ordinii.
OPERAȚII DE MENȚINERE A PĂCII	operații militare desfășurate cu acordul tuturor părților implicate, în scopul monitorizării și implementării unui acord urmărindu-se instaurarea unei stabilități politice de perspectivă.
OPERAȚII MILITARE ALTELE DECÂT RĂZBOIUL	activități în care instrumentul militar al puterii naționale este folosit pentru scopuri altele decât varietatea operațiilor însumate/asociate războiului, care urmăresc descurajarea războiului, rezolvarea conflictului, promovarea păcii și sprijinul autorităților civile în vederea soluționării crizelor interne.
OPERAȚII MULTINAȚIONALE	operații conduse de forțe aparținând mai multor națiuni care acționează împreuna pentru îndeplinirea unei singure misiuni.
OPERAȚIONAL	ceva sau cineva pregătit să intre în acțiune (activitate, operație); capacitatea optimă a formațiunilor (grupurilor, colectivelor) de a putea fi angajate în operație.
OPERAȚIONALITATE	proprietatea de a interveni prompt în rezolvarea unei probleme; calitatea organismelor de conducere (comandamente militare) de a fi capabile ca într-un termen relativ scurt să rezolve pe baza unor decizii, problemele multiple - atât în plan conceptual cât și acțional, pe timpul pregătirii și desfășurării acțiunilor militare.
OPERAȚIONALIZARE	întreprinderea unui summum de operații, adică totalizarea, cuantificarea și evaluarea lor alături de niște parametri la care trebuie să se ajungă pentru ca sistemele de conducere subordonate să devină operaționale.

OPERAȚIONALIZAREA STRUCTURILOR — principiu care asigură, prin aplicare sa, instrumentele prin care factorii de decizie politico-militară pun în mișcare sistemul, pentru a atinge pragul de reacție într-un interval de timp cât mai scurt.

OPERAȚIUNE DE PACE — acțiune militară de sprijinire a eforturilor diplomatice ale comunității internaționale pentru impunerea, menținerea sau restabilirea păcii și a securității în zonele de conflict.

ORDINE CONSTITUȚIONALĂ — starea în care se găsește ordinea publică într-un stat la un moment dat, modul de desfășurare a tuturor activităților și acțiunilor politice, sociale, economice și militare, având la bază Constituția și legile țării, respectiv modul în care sunt apărate drepturile omului și sunt executate îndatoririle cetățenești în vederea aigurării viabilității statului de drept.

ORGANIZAREA — funcție a conducerii care semnifică folosirea judiciaosă a resurselor umane și materiale în rezolvarea unor probleme concrete, utilizarea eficientă a resurselor; presupune armonizarea, stabilirea unor raporturi și proporții juste între categoriile de resurse.

ORGANIZAREA INSTRUCȚIEI ARMATEI — ansamblul de activități prin intermediul cărora se stabilesc sarcinile, pe structuri și posturi, necesare realizării obiectivelor propuse și are menirea de a pune în valoare următoarelor concepte: autoritatea, responsabilitatea, centralizarea sau descentralizarea sistemului de instrucție.

P

PARTICIPAREA LA APĂRAREA COMUNĂ — misiuni care se realizează prin pregătirea în cadrul unor exerciții cu participare internațională la acțiuni multinaționale și interaliate, precum și în structura unor mari unități și unități mixte, în scopul sporirii măsurilor de încredere și de securitate.

PERIOADĂ DE TENSIUNE — intervalul de timp în care inamicul potențial desfășoară, de regulă, acțiuni complexe de intimidare a statului român, concomitent cu obținerea acordului și a sprijinului internațional față de poziția și revendicările sale.

PLAN — document organizatoric necesar unei activități militare importante și complexe, cuprinzând totalitatea măsurilor de trebuie adoptate pentru atingerea obiectivelor fixate.

PLANIFICAREA — funcție a conducerii care reprezintă un ansamblu de acțiuni de complexitate variabilă, întreprinse în vederea determinării cât mai clar posibil a tuturor elementelor ce

caracterizează activitatea (procesul) condus și anume: obiective, subiect resurse (umane, materiale, financiare, informaționale), probleme de spațiu, timp, instrumente, metode și procedee utilizate. Reprezintă, de asemenea, stabilirea și fundamentarea obiectivelor și sarcinilor de realizare a acestora precum și a resurselor necesare pe o perioadă determinată, corespunzătoare obiectivului urmărit - lunar, trimestrial, anual.

PLANIFICAREA INSTRUCȚIEI ARMATEI — stabilirea obiectivelor și direcțiilor de acțiune în mod concret pe o anumită perioadă de timp în vederea folosirii eficiente a tuturor resurselor care stau la baza funcționării programului de instrucție a armatei.

PLURIFUNCȚIONALITATE — realizarea instrucției polivalente a militarului care să-i transfere capabilități acționale eficiente necesare îndeplinirii mai multor funcțiuni/posturi specifice armei/ specialității militare.

POTENȚIAL — termen care definește ceva, care are în sine toate condițiile esențiale pentru realizare, care există ca posibilitate, care există în mod virtual.

POTENȚIAL MILITAR — totalitatea forțelor și mijloacelor de luptă armată pe care un stat le poate afecta pregătirii și ducerii războiului.

PREDICȚIE — formulare de enunțuri ce descriu desfășurarea probabilă a unor fenomene și evenimente în virtutea cunoașterii dinamicii comportamentelor acestora.

PREGĂTIREA ACȚIUNILOR MILITARE — un ansamblu de activități și măsuri ce se execută de comandamente și de forțele subordonate acestora pentru conceperea și planificarea acțiunii, organizarea asigurării acțiunilor și protecției trupelor și logisticii, aducerea forțelor și mijloacelor la capacitatea de luptă necesară și în dispozitivele și situațiile optime, realizarea coordonării permanente a subordonaților și a cooperării neîntrerupte între toate forțele participante.

PREGĂTIREA DE FOC A ATACULUI — totalitatea acțiunilor de lovire ale aviației, artileriei, rachetelor și altor mijloace de foc executate în mod unitar, prin surprindere, într-o perioadă de timp stabilită, în scopul nimicirii sau neutralizării inamicului, îndeosebi în sectoarele de rupere și pe direcțiile de ofensivă ale marilor unități.

PREGĂTIREA DE FOC A OFENSIVEI — totalitatea acțiunilor categoriilor și sistemelor de armamente și mijloace de lovire (aviație, artilerie și rachete antiaeriene, artileria de pe navele maritime și

fluviale, tancuri) executării în scopul diminuării puterii de luptă și anihilării acțiunilor inamicului în spațiul terestru, maritim, aerian și fluvial, în special pe direcțiile de ofensivă. Aceasta se realizează astfel încât să se asigure lovirea la distanța mixima posibilă a mijloacelor de întrebuintare a armelor de nimicire în masă, sistemelor de cercetare-lovire de înalta precizie, punctelor de comandă și a grupărilor de forțe inamice aflate în raioane sau în deplasare.

PREVEDERE — deducere, intuire, întrezarire, bizuire asupra evoluției probabile a unui fenomen în perspectivă.

PREVENIREA, ÎNLĂTURAREA ȘI LICHIDAREA URMĂRILOR DEZASTRELOR — misiune care, în principal, vizează avestizarea populației, pregătirea acesteia pentru acțiune în diferite situații, elaborarea planurilor de evacuare și participarea cu forțe și mijloace la înlaturarea efectelor dezastrelor.

PREVENIREA CONFLICTELOR — activități care pornesc de la inițiativele diplomatice și până la desfășurarea preventivă a trupelor, în scopul prevenirii escaladării disputelor spre o fază superioară, aceea a conflictelor armate sau prevenirii extinderii disputelor.

PREVIZIUNE — prevedere întemeiată pe cunoașterea legilor obiective care guvernează evoluția probabilă a respectivului fenomen în perspectivă.

PREVIZIUNEA SISTEMULUI MANAGERIAL AL INSTRUCȚIEI — analizarea resurselor disponibile și gestionarea acestora în vederea stabilirii obiectivelor în domeniul instrucției armatei pe o perioadă de timp determinată având ca scopuri: stabilirea obiectivelor și scopurilor propuse; stabilirea sarcinilor și atribuțiilor pe structurile ce compun sistemul; stabilirea orientărilor și modul de coordonare a activităților de instruire în cadrul sistemului; prevederea disfuncționalităților ce pot apare în cadrul sistemului și măsurile corective ce trebuie adoptate pentru eliminarea acestora; stabilirea sistemului de control și modul de aplicare a prevederilor acestuia pentru îndeplinirea obiectivelor propuse.

PREZENȚA ÎNAINTATA — totalitatea activităților care demonstrează angajarea Armatei Române pentru consolidarea stabilității regionale, conferă credibilitate aliaților din care România face parte și sporesc posibilitățile de răspuns în cazul unei crize.

PRIMATUL — determină un anumit tip de ripostă a Forțelor Terestre,

LOVITURII	prin care se urmărește ca pe timpul desfășurării acțiunilor militare, în anumite circumstanțe ale situației operative care favorizează trupele proprii, să se execute lovituri decisive, preventive și prin surprindere, cu forțe strict limitate pentru devansarea și surprinderea în acțiune a adversarului.
PROCEDEU	prescripție privind ordinea operațiilor succesive de abordare a proceselor și fenomenelor în vederea organizării formale a datelor obținute și activităților.
PROCEDEU DE INSTRUCȚIE	modelul/felul de efectuare/executare a instrucției.
PROCEDURĂ DE STAT MAJOR	totalitatea măsurilor, activităților și documentelor elaborate/executate succesiv, pentru a ajunge la o decizie sau pentru a îndeplini o decizie din procesul executării actului de comandă.
PROGNOZA INSTRUCȚIEI ARMATEI	activitatea de cunoaștere și investigare în timp a etapelor pe care urmează să le parcurgă procesul de instrucție, având ca rezultat stabilirea obiectivelor de perspectivă și fundamentarea deciziilor în acest scop, în strânsă concordanță cu evoluția fenomenului militar mondial.
PROGNOZĂ	prevedere a desfășurării în timp a unui fenomen, a unui proces etc., bazată pe studiul împrejurărilor care îi determină apariția și evoluția; prevedere a valurilor pe care le vor lua în viitor unele mărimi din prezent.
PROGRAMARE DE INSTRUCȚIE	documente care cuprind obiectivele pe arme, categorii de instrucție, teme, exerciții și ședințe, atât la nivelul luptătorului cât și al subunităților/unităților, procedeele, regulile, standardele, resursele alocate precum și etapele/ perioadele/modulele și responsabilitățile privind conducerea și executarea instrucției.
PROTECȚIA	ansamblul de măsuri și acțiuni desfășurate continuu și într-o concepție unitară, de către toate forțele participante și la toate eșaloanele, destinate creării condițiilor de securitate a personalului, tehnicii și sistemelor împotriva acțiunilor agresorului și a altor factori perturbatori, executate în scopul menținerii capacității de luptă a trupelor și îndeplinirii misiunilor primite.
PROTECȚIA ANTIAERIANĂ	ansamblul măsurilor și acțiunilor întreprinse pentru prevenirea și apărarea grupărilor de forțe și a obiectivelor proprii împotriva cercetării aeriene și a loviturilor executate din aer de către agresor incusiv prin folosirea

mijloacelor nespecializate de luptă împotriva țintelor aeriene.

PROTECȚIA ELECTRONICĂ — ansamblul măsurilor și acțiunilor desfășurate unitar pentru asigurarea stabilității și a continuității lucrului mijloacelor și sistemelor electronice proprii. Se realizează prin respectarea regulior și regimului de lucru electronic propriu, mascarea și dezinformarea electronică, organizarea compatibilității electromagnetice între mijloacele (sistemele) electronice proprii, precum și prin decoperirea, neutralizarea și interdicția utilizării mijloacelor de luptă electronică ale inamicului.

PROTECȚIA GENISTICĂ — ansamblul măsurilor, acțiunilor și lucrărilor genistice care se planifică și execută de către toate forțele, în folosul propriu, pe timpul pregătirii și desfășurării acțiunilor, pentru crearea condițiilor necesare adăpostirii și protejării personalului și tehnicii împotriva loviturilor de orice gen ale inamicului și pentru îngreunarea și interzicerea acțiunii acestuia.

PROTECȚIA INFORMAȚIILOR — ansamblul măsurilor și acțiunilor organizatorice, informațioanle și tehnice luate și executate pentru respectarea regulilor de lucru în elaborarea și exploatarea documentelor, tehnicii și materialelor de conducere în secret și pentru păstrarea secretului, accesul autorizat și ierarhizat la date și informații, controlul informațiilor destinate publicului, protecția fizică și criptografică a informațiilor ce se transmit, disimularea informațională a inamicului, penetrarea documentelor de conducere în secret, cifrurilor și codurilor adversarului.

PROTECȚIA ÎMPOTRIVA MIJLOACELOR INCENDIARE — ansamblul de măsuri și acțiuni ce se desfășoară pentru protecția personalului împotriva efectelor armelor și munițiilor incendiare, limitarea și stingerea ingendiilor în dispozitivul trupelor și ieșirea din raioanele în care se produc incendii masive.

PROTECȚIA MEDICALĂ ȘI SANITAR-VETERINARĂ — ansamblul măsurilor și acțiunilor care se stabilesc și se desfășoară în vederea păstrării sănătății militarilor și animalelor, prevenirii apariției și răspândirii bolilor, inclusiv a celor provocate de armele de nimicire în masă.

PROTECȚIA PSIHOLOGICĂ — ansamblul de măsuri și acțiuni desfășurate într-o concepție unitară, pentru menținerea rezistenței și stabilității psihice a efectivelor proprii, ridicarea moralului acestora, identificarea și constracararea presiunilor psihice care afectează capacitatea de luptă și pentru influențarea psihologică a trupelor inamicului.

PUNCTUL DE COMANDĂ — locul de dispunere a personalului și mijloacelor comandamentului din care se exercită actul de comandă pe timpul pregătirii și desfășurării acțiunilor militare.

PUNCTUL DE COMANDĂ AJUTĂTOR — se poate crea pentru o perioadă de timp determinată mai ales la eșalonul corp de armată, în vederea conducerii unei grupări de forțe ce acționează pe o direcție izolată.

PUNCTUL DE COMANDĂ DE REZERVĂ — este destinat pentru întărirea stabilității, siguranței și continuității conducerii trupelor. El trebuie să fie pregătit pentru a prelua imediat și integral conducerea în cazul scoaterii din funcțiune sau a deplasării punctului de comandă.

PUTEREA DE LUPTĂ — componentă esențială a copacității combative specifică structurilor militare, exprimată integrator prin elementele capacității de distrugere a adversarului (puterea de lovire, conducerea, manevra, reacția și protecția).

PUTEREA MILITARĂ A FORȚELOR TERESTRE — una din componentele importante ale puterii militare a României, determinată în mod direct de posibilitățile națiunii de a o amplifica, regenera și redimensiona la nevoie. Se identifică prin: locul și rolul, efectivele (personalul militar), armamnetul și tehnica militară, structura organizatorică, coeziunea forțelor, starea și practica disciplinară, pregătirea pentru luptă a trupelor și capacitatea comandamentelor de a gândi, planifica, opera și acționa întrunit, inclusiv în structurile multinaționale.

R

RAIDUL — o operație mai restrânsă care implică o pătrundere rapidă în teritoriul ostil pentru obținerea de informații, dezorientarea adversarului sau distrugerea unor obiective și se încheie cu o retragere planificată.

RĂZBOI — fenomen politico-militar care reprezintă forma cea mai violentă de manifestare a relațiilor conflictuale existente la un moment dat între grupări mari de oameni (popoare, națiuni, state, coaliții de state, comunități sociale, etnice, religioase) organizate din punct de vedere militar, care folosesc lupta armată pentru atingerea scopurilor urmărite, ceea ce conferă acestui fenomen un puternic caracter distructiv.

RĂZBOI CLASIC (CONVENȚIONAL) — tip de război în care nu se folosesc armele de nimicire în masă ci numai mijloacele de luptă clasice. Lupta de succe numai cu forțe armate regulate, deosebindu-se în acest fel de războaiele duse cu forțe armate neregulate (miliții, guerile, partizani etc.).

RĂZBOI DE INTENSITATE REDUSĂ	concepție de ducere a războiului care nu presupune victoria, ci reducerea graduală a violenței printr-un control relativ al conflictului pe baza unui instrument pluridimensional social.
RĂZBOI LIMITAT	tip de război prin care se încearcă evitarea riscurilor și consecințelor unui război nuclear total, introducându-se o serie de limitări în ceea ce privește scopurile urmărite, armele întrebuințate și teatrul de acțiuni militare.
RĂZBOI MANEVRIER (DE MIȘCARE)	tip de război în care predomină acțiunile manevriere, fiecare dintre beligeranți urmărind obținerea deciziei prin operații cu caracter mobil.
RĂZBOI MODERN	acel conflict armat care adoptă principii noi, ca rezultat al unor interdependențe între evenimentele de natură conflictuală, apariția unor noi armamente și tehnici de luptă și, în sfârșit, o alegere sau o compunere a acțiunilor, altele decât în războaiele desfășurate sau în curs de desfășurare.
RĂZBOI PUTERNIC DEMASIFICAT	tip de război preconizat să se desfășoare cu efective reduse (profesioniști), înzestrate cu sisteme de armament și tehnică de luptă moderne, performante.
RĂZBOI TOTAL	tip de război în care se urmărește distrugerea totală a adversarului și se folosește în acest scop totalitatea mijloacelor de luptă.
REACȚIE RAPIDĂ	termen prin care se justifică o acțiune rapidă condiționată de un pretext sau o modalitate de a concepe reacția unei armate sau a unei grupări de forțe.
REGRUPAREA	acțiunea prin care se realizează o nouă grupare a forțelor și mijloacelor în scopul îndeplinii aceleiași misiuni sau a uneia noi.
RELAȚII DE COOPERARE	totalitatea activităților desfășurate de structurile Ministerului Apărării Naționale într-o concepție unitară pentru asigurarea resurselor, planificarea, organizarea, îndrumarea, controlul și evaluarea sistemului de instrucție al armatei.
RESTABILIREA ORDINII CONSTITUȚIONALE	ansamblul măsurilor și acțiunilor întreprinse de către organele și forțele legale ale statului destinate pentru repunerea acesteia în drepturile ei firești, atunci când a fost grav tulburată.
RESURSA	suma alocată armatei din bugetul statului pentru

FINANCIARĂ (A INSTRUCȚIEI) instrucție, cu implicații determinate în planificarea obiectivelor și scopurilor ce trebuie îndeplinite într-o unitate de timp.

RESURSA MATERIALĂ (A INSTRUCȚIEI) totalitatea materialelor pentru instrucție, a echipamentelor, utilajelor și tehnicii din dotare, precum și a infrastructurii necesare instrucției (poligoane, piste, servicii etc.) care, palnificate și folosite în mod judicios constribuie la instrucția trupelor din structurile armatei, conform programului stabilit.

RESURSA UMANĂ personalul de decizie și execuție din sistemul de instrucție prin care se asigură realizarea documentelor care stau la baza instrucției armatei și punerea în practică a prevederilor acestora, concomitent cu planificarea și gestionarea resurselor materiale și financiare.

RESURSĂ (A INSTRUCȚIEI) element de bază, fără de care sistemul de instrucție al armatei nu poate să-și atingă scopul pentru care a fost înființat și constă în totalitatea posibilităților pe care le are societatea la un moment dat de a pune la dispoziția armatei efectivele, baza materială și financiară necesară instrucției în conformitate cu obiectivele stabilite.

RESURSE MILITARE ansamblul forțelor și mijloacelor specializate pentru lupta armată, pe care staul român le poate destina pregătirii și ducerii războiului, dacă acesta este impus și anume: efectivele și tehnica de luptă; numărul și calitatea cadrelor de comadă, organizarea și coeziunea forțelor armate; nivelul pregătirii populației pentru apărare; gradul de dezvoltare a științei și artei militare.

RESURSELE APĂRĂRII NAȚIONALE totalitatea posibilităților umane, financiare, materiale și de altă natură de care staul român dispune și pe care le poate angaja în susținerea efortului de apărare a țării.

RETRAGEREA procedeul defensiv prin care forțele angajate în luptă întârzie acțiunile inamicului și se sustrag loviturilor puternice ale acestuia, schimbându-și pozițiile de luptă spre înapoi.

REZERVA element component al dispozitivului de luptă întrebuințat pentru rezolvarea unor situații critice neprevăzute care pot să apară pe timpul desfășurării operației. Se constituie din mari unități (unități), din toate categoriile de forțe ale armatei, din arme și specialități, în funcție de existentul acestora, complexitatea situațiilor și caracteristicile geoclimatice ale zonei.

REZERVE STRATEGICE totalitatea resurselor militare, economico-financiare, demografice, tehnologice și materiale care se constituie la nivel statal și al eșaloanelor militare strategice ce se întrebuințeaza în caz de război sau de criză (catastrofe naturale sau ecologice) în vederea rezolvării unor situații neprevăzute sau a amplificării (intensificării) acțiunilor militare în curs de desfășurare.

RIPOSTĂ ansamblul de acțiuni spațiale și acționale în teritoriul adversarului, care includ totalitatea atitudinilor ofensive, defensive și pasive ale unei categorii de forțe ale armatei.

RIPOSTĂ ARMATĂ DEFENSIVĂ o atitudine strategică, o modalitate de a respinge agresiuni armate printr-o apărate strategică flexibilă și activă, în cadrul căreia se va folosi întreaga gamă a procedeelor de ducere a operațiilor care permit, în final, într-o conjunctură poliitico-militară favorabilă, realizarea integrală a obiectivului politico-strategic al războiului de apărare a țării.

RIPOSTĂ OFENSIVĂ acțiune ofensivă în cadrul apărării prin care se urmărește nimicirea inamicului pătruns în interiorul apărării și refacerea acesteia pe aliniamentul inițial (riposta de răspuns) sau lovirea inamicului în fața limitei dinainte apărării (riposta de prevenire).

RIPOSTĂ OPTIMĂ principiul fundamental al acțiunilor militare în caz de război, similar „apărării flexibile și ripostei ofensive decisive".

RITM viteza cu care se realizează, într-o perioadă dată anumite acțiuni de luptă sau alte activități militare.

RUPEREA APĂRĂRII acțiune de luptă dusă împotriva unui inamic aflat în apărare, incluzând executarea loviturii frontale și crearea unei breșe în dispozitivul apărării inamice, de o lărgime și adâncime care să permită dezvoltarea ulterioară a ofensivei în adâncime și spre flancuri.

S

SCOPUL STRATEGIC GENERAL AL APĂRĂRII ARMATE A ȚĂRII constă în respinderea, capturarea ori nimicirea grupărilor de forțe ale agresorului și anihilarea capacității combative a acestuia, urmărindu-se asigurarea suveranității naționale, independenței și unității statale, integrității teritoriale a țării.

SECURITATEA NAȚIONALĂ	starea în care trebuie să se găsească statul român pentru a putea să se dezvolte liber și să acționeze neîngrădit pentru promovarea intereselor fundamentale ale României.
SIMULARE CONSTRUCTIVĂ	formă de instrucție specifică pregătirii comezilor și comandamentelor de la nivel batalion până la nivel teatru de operații, ce se realizează prin antrenamente de stat major/aplicații de comandament asistate de calculator.
SIMULARE ÎN TEREN CU TRUPE	forma de instrucție cea mai complexă care asigură instruirea militarilor, subunităților, comenzilor și comandamentelor prin exerciții și aplicații tactice în teren, în cele mai apropiate condiții impuse de câmpul de luptă modern, fără utilizarea munițiilor de război.
SIMULARE VIRTUALĂ	formă de instrucție care asigură instruirea militarilor și echipajelor prin utilizarea machetelor electronice ale tehnicii de luptă.
SISTEM	ansamblul de elemente (principii, reguli, forțe etc.) dependente între ele și formând un întreg organizat care face ca o activitate practică să funcționeze potrivit scopului urmărit.
SISTEM DE CONDUCERE	ansamblul de metode, tehnici și instrumente, asociat cu procedurile informaționale, decizionale și organizatorice specifice metodelor și tehnicilor integrate în cadrul sistemului.
SISTEMUL DE CONDUCERE A FORȚELOR TERESTRE	parte componentă a sistemului de conducere a armatei, destinată să facă posibilă conlucrarea și cooperarea cu structurile de comadă din compunerea Ministerului Apărării Naționale, Statul Major General, statelor majore ale categoriilor de forțe ale armatei, celorlalte elemente ale Sistemului Național de Apărare, administrației locale, precum și din cea a partenerilor de coaliție sau de misiuni comune.
SISTEM DE LOVIRE	ansamblul acțiunilor tuturor categoriilor și sistemelor de armamente și mijloace de lovire, executate în scopul producerii de pierderi, diminuării puterii de luptă și anihilării acțiunilor inamicului, în spațiul terestu, aerian, maritim și fluvial.
SPRIJIN LOGISTIC	orice ajutor sub formă de bunuri și/sau servicii, sprijin tehnic sau nontehnic, acordat de o parte ce oferă sprijin către o parte primitoare.

SPRIJINUL CIVIL	totalitatea activităților și măsurilor luate de forța de intervenție în scopul favorizării asistenței și sprijinului reciproc între structurile militare și orice organism civil în procesul de planificare/pregătire sau aplicare a resurselor necesare pentru a răspunde consecințelor unor situații critice, de urgență, de natură civilă sau în caz de atac, incluzând situațiile de urgență în planul securității naționale.
SPRIJINUL INSURGENȚILOR	operație care asigură sprijinirea unei mișcări organizate care urmărește unui grup constituit pe calea subversiunii și a conflictului armat.
STANDARD	o valoare, o unitate fizică sau o noțiune abstractă, stabilită și definită de autoritate, obicei sau acord comun pentru a servi ca referință, model sau regulă în măsurile cantitative sau calitative, în stabilirea practicilor ori procedurilor, sau în evaluarea rezultatelor.
STANDARD DE INSTRUCȚIE	normele, baremele, criteriile sau ansamblurile de norme care sunt stabilite pentru un agent al acțiunii militare sau pentru o structură militară care îndeplinesc o acțiune/ activitate/misiune specifică în anumite condiții.
STANDARDE OPERAȚIONALE	cele ce fac referință asupra practicilor, procedeelor, metodelor, cu aplicabilitate imediată sau viitoare. Ele privesc: aspectele de natură conceptuală, doctrinară, tactică și tehnică; antrenamentele, pregătirea și perfecționarea; precizările organizatorice, rapoartele, schemele, hărțile ș.a.
STANDARDIZARE	procesul de formulare (elaborare), punere de acord și introducerea standardelor în cadrul Alinației NATO în scopul dezvoltării capacității ei militare.
STANDARDIZAREA LOGISTICĂ	procesul dezvoltării conceptelor, procedeelor și proiectelor de a realiza și menține nivelurile cele mai adecvate de compatibilitate, interoperativitate, interschimbabilitate și a calității de a fi comune în domeniul operațiilor, administrației și materialelor.
STAREA DE CRIZĂ	situația în care sistemul social-global, în totalitate sau numai parte din el, este marcat de convulsii, de amenințări interne și externe sau mixte, precum și de stagnarea și perturbarea vieții societății, toate acestea punând în pericol valorile naționale și democrația constituțională.
STAREA DE PACE	cadrul de normalitate relativă, în care viața economică, politică, militară etc. își urmează cursul firesc.

STATUL MAJOR AL FORȚELOR TERESTRE	structură de comandă, de concepție și execuție care răspunde de întrebuințarea forțelor și mijloacelor din subordine, funcționează la pace, în situații de criză și război și se subordonează ierarhic Statului Major General.
STAȚIONAREA	acțiunea pe care o desfășoară structurile militare atunci când nu execută operații militare, nu se deplasează și nu sunt în dispozitiv de luptă.
STRATEGIE	ansamblul de concepte și măsuri ce constau în aplicarea resurselor naționale, diplomatice; economice și militare, pentru îndeplinirea obiectivelor politice.
STRATEGIILE INSTRUCȚIEI ARMATEI	programele generale/direcțiile de acțiune/alocare a resurselor pentru executarea intrucției pe termen mediu/ lung. Ele stabilesc obiectivele, definesc responsabilitățile, asigură ghidul/îndrumarile/metodologiile și repartizează prioritățile.
STRATEGIILE INSTRUCȚIEI FORȚELOR TERESTRE	programele generale/direcțiile de acțiune/alocare a resurselor pentru executarea intrucției pe termen mediu/ lung; sunt elaborate de către Statul Major General al Forțelor Terestre și sunt materializate prin regulamente, instrucțiuni, dispoziții și manuale ce cuprind prevederi generale sau specifice privind executarea instrucției.
SUBSISTEMUL DE PROTECȚIE	totalitatea forțelor și mijloacelor care au misiunea de a asigura securitatea sistemului de conducere și vizează sursele, mijloacele de prelucrare, suporții, legăturile, depozitele, locurile de afișare-exploatare și purtătorii de informații.
SUBSISTEMUL INFORMAȚIONAL	totalitatea forțelor și mijloacelor din structura Forțelor Terestre cu ajutorul cărora sunt obținute, transmise, prelucrate, depozitate și exploatate informații, date și semnale.
SUBSISTEMUL INFRASTRUCTURII	totalitatea comandamentelor de mari unități (la pace și în situații de criză) și a punctelor de comandă.
SUBSISTEMUL MANAGERIAL	cuprinde modulele (centrele operaționale) ale punctelor de coamdă (comandamentelor), reguli de funcționare și relațiile dintre acestea.
SUFICIENȚA ACTIVĂ A APĂRĂRII	structură de potențial, stațial și temporal, subsumată nivelului global, cu coeficient al stării de resursă activă, în măsură să asigure riposta armată pentru respingerea din primele momente ale unui tip de agresiune pe o direcție strategică.

SUFICIENȚA PENTRU APĂRARE (PRINCIPIU) concept strategic fundamental care reflectă opțiunea statului român în domeniul apărării, semnifică tipologia exclusiv defensivă a războiului ca model strategic preconizat pentru respingerea unei agresiuni și desemnează starea de normalitate a Sistemului Național de Apărare, fără a reprezenta o amenințare la adresa altor state.

SURPRINDEREA are rolul de a impune adversarului voința proprie, de a realiza superioritatea în punctul și la momentul hotărâtor. Odată realizată, paralizează capacitatea de reacție cel puțin la nivelul eșalonului direct afectat, inclusiv la nivelul conducerii, care nu mai reacționează în timp oportun pentru contracararea adversarului.

SURPRINDEREA STRATEGICĂ ansamblul măsurilor și acțiunilor adoptate de conducerea politico-militară în cadrul unei operații strategice sau uneori al unei campanii ori a unei etape a războiului, în așa fel încât acțiunile politice, militare, diplomatice, economice, pshilogice etc. atât în ceea ce privește conținutul (substanța), cât și în ceea ce privește locul, momentul, amploarea, procedeele practice de acțiune (realizare), să aibă un caracter neprevăzut pentru adversar.

Ș

ȘEDINȚĂ PRANCTICĂ formă de organizare a procesului de instrucție ce asigură formarea deprinderilor individuale de bază ale luptătorilor, a deprinderilor colective specifice grupelor/similare, a capacității de rezolvare a situațiilor complexe, neprevăzute, în timp oportun a evenimentelor apărute în dinamica luptei.

ȘEDINȚA PRACTIC-APLICATIVĂ formă de organizare a procesului de instrucție care se execută, de regulă, întrunit cu subunitatea și unitatea urmărindu-se, pe lângă realizarea obiectivelor punctuale, în mod deosebit, închegarea acțiunilor subunităților și unităților, precum și intruirea integrată de la cel mai mic nivel, respectiv echipa/postul/echipajul/similare, până la nivelul batalionului/similare.

ȘEDINȚĂ TEORETICĂ formă de organizare a procesului de instrucție care asigură însusirea conceptelor, a limbajului militar, a informațiilor despre acțiunile ce urmează să fie învatate, a cunoștințelor necesare formării atitudinilor și sentimentelor superioare

T

TEHNICA DE CONDUCERE — ansamblul de reguli specifice, procedee și instrumente prin care se soluționează concret probleme ce decurg din funcțiile conducerii.

TERORISMUL — un act violent premeditat, realizat de organizații conspirative cu caracter distructiv sau de persoane individuale, împotriva unor demnitari, a unor obiective (instituții) politice, economice, științifice, militare, culturale, diplomatice, în scopul răzbunării, obligării țintei să adopte o conduită convenabilă teroriștilor, sensibilizării opiniei publice în legătură cu o cauză anumită, al erodării stabilității politice și satisfaceerii unor revendicări.

TRANSPORTUL — deplasarea organizată a structurilor militare pe vehicule, altele decât cele din dotarea proprie.

TRANSPORTURILE LOGISTICE — activitățile desfășurate pentru deplasarea materialelor din sursele de aprovizionare până la luptător (tehnică), precum și a celor care prisosesc pe câmpul de luptă, către înapoi, în locurile stabilite din timp.

U

UNITATEA CONDUCERII ȘI RĂSPUNDERII — stabilirea precisă a atribuțiilor și responsabilităților pe sfere și niveluri de activitate, începând cu structurile cele mai mici până la structura care coordonează sistemul de instruire al armatei.

UNITATEA DE EFORT — derivă din principiul unității de comandă și cere ca în fiecare operație militară toate mijloacele să fie întreptate spre un obiectiv comun.

Z

ZONĂ DE INFLUENȚĂ — spațiul geografic care include statele și regiunile a căror evoluție influențează direct situația din țara noastră și cuprinde în esență țările vecine și Marea Neagră.

ZONĂ DE INTERES — spațiul din afara zonei de responsabilitate care cuprinde factori ce pot influența pregătirea și desfășurarea acțiunilor militare.

ZONĂ DE RESPONSABILITATE — spațiul în care comandantul unei unități are responsabilitatea pentru amenajarea genistică, controlul deplasărilor și conducerea acțiunilor militare ale forțelor subordonate, precum și autoritatea necesară pentru măsurile de rezolvare ale acestora.

ZONĂ LOGISTICĂ — porțiune de teren destinată marilor unități strategice sau operative pentru dispunerea și desfășurarea acțiunilor marilor unități, unităților și formațiunilor de logistică, stabilirea responsabilităților în folosirea căilor de comunicație, organizarea folosirii posibilităților logistice ale zonei și aplicare unitară a măsurilor de protecție.

CUPRINS

PREFAȚĂ 7

BAZELE RĂZBOIULUI INFORMAȚIONAL 9
Era informației 9

RĂZBOIUL INFORMAȚIONAL DEFENSIV 29

OPERAȚIILE INFORMAȚIONALE.
CÂTEVA REFLECȚII OPERAȚIONALE SISTEMUL SISTEMELOR 66

ATACUL INFRASTRUCTURII CRITICE 94

RĂZBOIUL NEOCORTICAL UN CONCEPT PENTRU VIITOR 118

OPERAȚIILE INFORMAȚIONALE PERSPECTIVA NATO 129

A INFORMA, CHIAR ÎN CONDIȚII DIFICILE.. 143

SIGURANȚA INFORMAȚIONALĂ 150

EXPLOZIA TEHNOLOGIEI INFORMAȚIEI 177
Dimensiunea 1: Conținutul 183
Dimensiunea 2: Intervalul de timp 185
Dimensiunea 3 : Accesibilitatea 187
Dimensiunea 4: Gradul de încredere 187
Dimensiunea 5 : Calitatea 188
Dimensiunea 6: Cantitatea 188

STUDIUL GERMANO-OLANDEZ DESPRE RĂZBOIUL INFORMAȚIONAL 196
RĂZBOIUL INFORMAȚIONAL PROBLEME și PERSPECTIVE 213
EXCURS IN SPAȚIUL CONCEPTELOR 214
RĂZBOIUL INFORMAȚIONAL. ABORDARE TEORETICĂ 217
ȚINTE ȘI ELEMENTE ALE UNUI ATAC INFORMAȚIONAL 225
INFRASTRUCTURILE CRITICE ÎN RĂZBOIUL

INFORMAȚIONAL 229
PROBLEMATICA EVALUĂRII AMENINȚĂRILOR 233
RĂZBOIUL INFORMAȚIONAL ȘI LEGISLAȚIA INTERNAȚIONALĂ 236

VULNERABILITĂȚI ALE TEHNOLOGIEI INFORMAȚIEI 241

OPERAȚIILE INFORMAȚIONALE UN MIJLOC DE DESCURAJARE STRATEGICĂ 265
DELIMITĂRI SI DIFERENTE 268
FORMELE DEFENSIVE ȘI OFENSIVE ALE OPERAȚIILOR INFORMAȚIONALE 270
MANAGEMENTUL PERCEPȚIILOR ȘI FACTORUL UMAN 274
ELEMENTE ALE UNEI STRATEGII DE INFLUENȚARE 278
SIGURANȚA INFORMAȚIONALĂ EXPERIENȚA CANADIANĂ 291
RĂZBOIUL INFORMAȚIONAL PROBLEME DE SECURITATE 304
RĂZBOIUL CUNOAȘTERII 334
REVOLUȚIA INFORMAȚIONALĂ 353

Anexa 1: NETWORK CENTRIC WARFARE 373

Anexa 2:
1. RĂZBOIUL INFORMAȚIILOR A DEVENIT DEJA O REALITATE A CÂMPULUI DE LUPTĂ MODERN 413
2. CARACTERISTICI ALE DINAMICII RESURSELOR INFORMAȚIONALE 418
3. OPERAȚIILE INFORMAȚIONALE 420
4. OPERAȚIILE INFORMAȚIONALE PENTRU SITUAȚIILE DE URGENȚĂ 432
5. RĂZBOIUL MEDIATIC 434
6. RĂZBOIUL ELECTRONIC 449
7. TERORISMUL INFORMATIC 455

Anexa 3: Resurse URL (Uniform Resourse Locator) 465

Dicționar 471